NetScaler Intelligent Traffic Management

Machine translated content

Disclaimer

Contents

Novedades

April 29, 2022

Nueva función/mejora	Versión
Alertas: Esta función supervisa los problemas o anomalías de rendimiento de las plataformas configuradas desde una red de usuario final en todo el mundo.	2022.02.15
Persistencia local: Esta función ofrece la capacidad de mantener la firmeza de las decisiones cuando está habilitada. Las solicitudes se identifican mediante la máscara de subred IP, cuya longitud se puede configurar. Por ejemplo, cuando un cliente repite una solicitud a la misma aplicación dentro de un período determinado (TTL de persistencia), se devuelve la decisión original.	2021.12.09
Conector de ELB de AWS: Este nuevo conector extrae las métricas `HealthyHostCount`, `UnHealthyHostCount` y `Load Balancer Capacity Units (LCUs)` de AWS ELB a través de Fusion. Proporciona a los clientes una experiencia integrada de equilibrio de carga y visibilidad de las métricas de Fusion disponibles en sus aplicaciones Openmix.	2019.08.16
Cambiar el tipo de plataforma (privada a comunitaria): esta nueva función permite a los clientes cambiar la configuración actual de su plataforma privada o GSLB para hacer referencia a la plataforma de la comunidad. Esta función es útil para los clientes cuyas plataformas privadas están alojadas en un centro de datos público o en una región de la nube.	2019.07.03

Nueva función/mejora	Versión
Nuevo panel de control: El nuevo panel de control de ITM ahora está operativo, tiene mucha información, es personalizable y, en general, es más útil que la versión anterior. En el nuevo panel de control, puede ver las tablas de sesiones de radar, rendimiento del radar, decisiones de gestión del tráfico de Openmix y estado de supervisión de sonda. Puede crear varios paneles, cada uno adaptado a una vista que le importe. También puede optar por convertir el Visualizador ITM o el Panel de control en su página de destino predeterminada.	2019.06.27
Cuarentena de fusión: esta función pone en cuarentena la fuente de datos de Fusion defectuosa de un cliente, si la fuente falla o se ejecuta en un intervalo de sondeo inferior a 24 horas. Fusion aplica la lógica de cuarentena para evitar que se ejecuten estas fuentes con errores para ahorrar recursos (CPU/memoria) y evitar el impacto en otras fuentes de datos de Fusion válidas o válidas.	2019.06.19
Habilitar/inhabilitar plataformas para Openmix: Ahora se puede habilitar o inhabilitar una plataforma para Openmix activando o desactivando el botón **Openmix Enabled** en Configuración de plataforma. Si una plataforma en particular está inhabilitada para Openmix, esa plataforma no se tendrá en cuenta en las decisiones de Openmix.	2019.04.09

Nueva función/mejora	Versión
Plataforma geográfica: Esta función permite a los clientes ver y administrar la ubicación geográfica asignada a una plataforma. De forma predeterminada, no hay ninguna ubicación **geográfica** asignada a las plataformas privadas. Cuando un usuario crea una plataforma privada y configura un sondeo Radar, usamos la URL del sondeo para localizar la plataforma. Alternativamente, el usuario puede asignar un Geo manualmente sin depender de la ruta URL del Radar. Para las importaciones de configuración GSLB y F5, localizamos la IP pública y la usamos como el **Geo** de la plataforma. Las plataformas comunitarias heredan de forma predeterminada la ubicación original de la plataforma.	2019.04.09
Visualizador: Profundice al nivel estatal: alertas activas con información sobre el rendimiento y la disponibilidad de las nubes, los centros de datos, las CDN y otros servicios. Estas alertas se miden y se ven a nivel estatal dentro de los Estados Unidos.	2019.04.01
Visualizador: importaciones de F5 y GSLB - Importaciones de F5 y GSLB: ahora puede importar una plataforma a través de una configuración de GSLB o F5. La información básica del sitio (IP y nombre) se importa como plataformas ITM. ITM geolocaliza el sitio y permite que la plataforma se muestre en el visualizador para el análisis del rendimiento.	2019.03.29
Adaptador de purga G-Core: El adaptador de purga CDN G-Core ahora se agrega a la lista de adaptadores que ITM admite para ejecutar purgas.	2019.03.29

Nueva función/mejora	Versión
Radar DSA 3 para todos los proveedores de la comunidad: Para mejorar continuamente la comunidad de Radar y la precisión de nuestros puntos de referencia, recientemente lanzamos un nuevo Dynamic Content Benchmark. Este nuevo banco de pruebas tiene una página HTML dinámica y una firma con la que se puede verificar la medición.	2019.03.21
Visualizador: El visualizador ITM es una herramienta intuitiva e inteligente que le permite supervisar y analizar el rendimiento global de los ISP y los servicios. La interfaz de usuario del visualizador de ITM proporciona alertas activas con información sobre el rendimiento y la disponibilidad de las nubes, los centros de datos, las CDN y otros servicios. La comunidad de ITM mide estas alertas en todo el mundo. ITM Radar recopila miles de millones de mediciones de usuarios reales de todo el mundo a través de la comunidad de Radar. Utiliza un modelo de crowdsourcing para medir estas alertas.	2019.03.08
Las visitas guiadas (visitas guiadas) para el Visualizador y Openmix ya están disponibles en el **portal de demostración de ITM**. Se puede acceder al Portal Demo a través del icono de ayuda dentro del portal ITM. En la esquina inferior derecha del **Portal Demo** se muestra un icono que inicia las visitas guiadas.	2019.03.08

Notificaciones de terceros

September 13, 2023

Notificaciones de terceros de NetScaler Intelligent Traffic Management (PDF)

Glosario

September 13, 2023

Término	Descripción
Aplicación	Una aplicación Openmix es una especificación de lógica de equilibrio de carga que se puede configurar dentro del portal. La aplicación se procesará para cada solicitud realizada a Openmix y se tomará una decisión de enrutamiento basada en la lógica especificada. Las aplicaciones se pueden utilizar para uno o varios tipos de contenido. Un cliente puede tener una aplicación para un tipo de contenido que tiene un alto valor para el negocio y una aplicación diferente para el contenido que tiene un valor menor que debe enrutarse de manera diferente. Por ejemplo, el cliente puede tener una aplicación de contenido mostrada a todos los usuarios que se centra en enrutar al proveedor más rápido independientemente del coste. El cliente también puede tener otra aplicación para contenido que rara vez se muestra que se centra en la optimización de costes entre proveedores para contenido de menor valor. En el escenario anterior, el cliente tendría dos aplicaciones Openmix.

Término	Descripción
Medidas comunitarias	Las mediciones de la comunidad se obtienen a través de un modelo de aprovisionamiento multitudinario que proporciona al cliente una visión del rendimiento y la disponibilidad de un proveedor a nivel geográfico y lógico a nivel global. Las medidas comunitarias están disponibles de forma gratuita para los miembros de la comunidad participantes (se requiere la instalación de la etiqueta JavaScript). El acceso a los datos de la comunidad para organizaciones que no contribuyen (es decir, que no integran JS) es un elemento facturado.
Decisión	Una decisión de Openmix se especifica como una solicitud única a uno de los balanceadores de carga de NetScaler. Para DNS, se trata de una única solicitud DNS a los equilibradores.Para HTTP, se trata de una solicitud GET o HEAD al extremo HTTP de Openmix.
Medición	Una medición se refiere a Radar y la recopilación de datos de los usuarios finales sobre el desempeño de una aplicación de servicio. Para mediciones de la comunidad, consulte Medidas de la comunidad.
Plataforma	Una plataforma es un CDN, nube, centro de datos u otro punto final que el cliente desea monitorizar dentro de Radar o utilizar dentro de la aplicación Openmix.
Medición privada	Las mediciones privadas de Radar son donde las mediciones o la telemetría (en el caso de la transmisión) se alimentan de la experiencia de los usuarios finales que no se comparte con la comunidad. Esto puede aplicarse cuando un cliente está buscando medir: + Su propia arquitectura de centro de datos + Uso de su propio objeto de prueba o página + Uso de su propio contrato con un proveedor + Calidad de experiencia para el usuario final de audio/vídeo

Definiciones de datos de Radar

June 4, 2021

Los socios de referencia y los miembros de la comunidad de Radar que han implementado la etiqueta de Radar pueden tener acceso opcionalmente a sus mediciones de Radar. En el caso de los socios de referencia, compartimos las mediciones tomadas de ese socio independientemente de la página en la que se implementó la etiqueta de Radar o cuándo se realizó la medición. Los miembros de la comunidad pueden ver todas las mediciones, tomadas por sus visitantes de la web, independientemente del socio de referencia que se esté midiendo.

Compartir datos de Radar del cliente

Los implementadores de etiquetas de Radar pueden acceder opcionalmente a un subconjunto de los campos que recibimos del cliente de Radar cuando se toma una medición de Radar en su sitio web. Las direcciones IP de los usuarios se anonimizan antes de generar los informes. Para obtener descripciones de registros, consulte la documentación de Netscope (NEM).

Mediciones Raw Radar

Las mediciones Raw Radar contienen un subconjunto de los campos que recibimos del cliente Radar cuando se realiza una medición Radar. Las direcciones IP de los usuarios se anonimizan antes de generar los informes.

Los informes pueden estar disponibles diariamente o en tiempo real que entregan datos de medición en menos de 5 minutos.

Los archivos pueden ser delimitados por TAB, CSV o formato JSON. Para obtener descripciones e informes de registro, consulte la documentación de Netscope.

Números de sistema autónomo

https://s3-eu-west-1.amazonaws.com/community-radar/ref/asns.json.gz

ID de proveedor (público) de la comunidad

https://s3-eu-west-1.amazonaws.com/community-radar/ref/providers.json.gz

Tipos de sonda (Tipos de medición)

https://s3-eu-west-1.amazonaws.com/community-radar/ref/probetypes.json.gz

---

Códigos de respuesta

Código	Módulo	Descripción	Valor
0	Todo	Operación correctamente realizada.	Valor de medición
1	Sondeo remoto	Tiempo de espera de solicitud HTTP	0
2	Sondeo remoto	Error en la conexión RTMP	0
3	Sondeo remoto	No se encontró la secuencia RTMP	0
4	Sondeo remoto	Archivo HTTP no válido	0
5	Temporización de navegación	No se admite la API de sincronización de navegación	0

Códigos de mercado

Código	Nombre	Abreviatura ISO
0	Desconocido	XX
1	América del Norte	NA
2	Oceanía	OC
3	Europa	UE
4	Asia	AS
5	África	AF
6	América del Sur	SA

Códigos de país

Basado en ISO 3166 -1 Alfa 2

https://s3-eu-west-1.amazonaws.com/community-radar/ref/countries.json.gz

Códigos de región

No existen normas ISO para las regiones que conocemos. Además, nuestro proveedor GEO proporciona regiones solo para un pequeño subconjunto de países. Según sus documentos, el objetivo de las "regiones"es subdividir ciertos países en áreas más grandes que los Estados. Por ejemplo, "EE. UU. - Suroeste"

Para empezar, proporcionamos nuestros propios "ID de región"numéricos y una asignación: https://s3-eu-west-1.amazonaws.com/community-radar/ref/regions.json.gz

> **NOTA:** Nos reservamos el derecho de cambiar el formato de ese archivo. Cualquier código creado para cargar en esas asignaciones debe crearse teniendo esto en cuenta. A largo plazo habrá una llamada a la API para descargar estas asignaciones.

Códigos de Estado

Existe un estándar ISO para estados 3166-2. Estamos evaluando si este estándar satisface nuestras necesidades. Así que empezar, estamos utilizando nuestra propia asignación numérica para cadenas. Similar a la región, el formato puede cambiar https://s3-eu-west-1.amazonaws.com/community-radar/ref/states.json.gz

Códigos de ciudad

Estamos utilizando nuestras propias asignaciones numéricas para cadenas. Similar a la región, el formato puede cambiar y eventualmente podemos proporcionar estas asignaciones como una llamada a la API. https://s3-eu-west-1.amazonaws.com/community-radar/ref/cities.json.gz

Visualizador

September 13, 2023

Introducción

El visualizador ITM es una herramienta intuitiva e inteligente que le permite supervisar y analizar el rendimiento global de los ISP y los servicios. La interfaz de usuario del visualizador de ITM proporciona alertas activas con información sobre el rendimiento y la disponibilidad de las nubes, los centros de datos, las CDN y otros servicios. La comunidad de ITM mide estas alertas en todo el mundo. ITM Radar recopila miles de millones de mediciones de usuarios reales de todo el mundo a través de la comunidad de Radar. Utiliza un modelo de crowdsourcing para medir estas alertas.

Para un nuevo usuario, la página del visualizador se abre con todas las alertas de comunidad disponibles en el mapa. ITM Radar mide las anomalías de rendimiento y genera alertas en casi todas las redes y en todas las ubicaciones del mundo.

Los cuatro iconos sobre el mapa Visualizer muestran los siguientes datos.

Alertas de Radar activas

Las alertas de Radar Activo son actuales y en curso.

Alertas de Radar

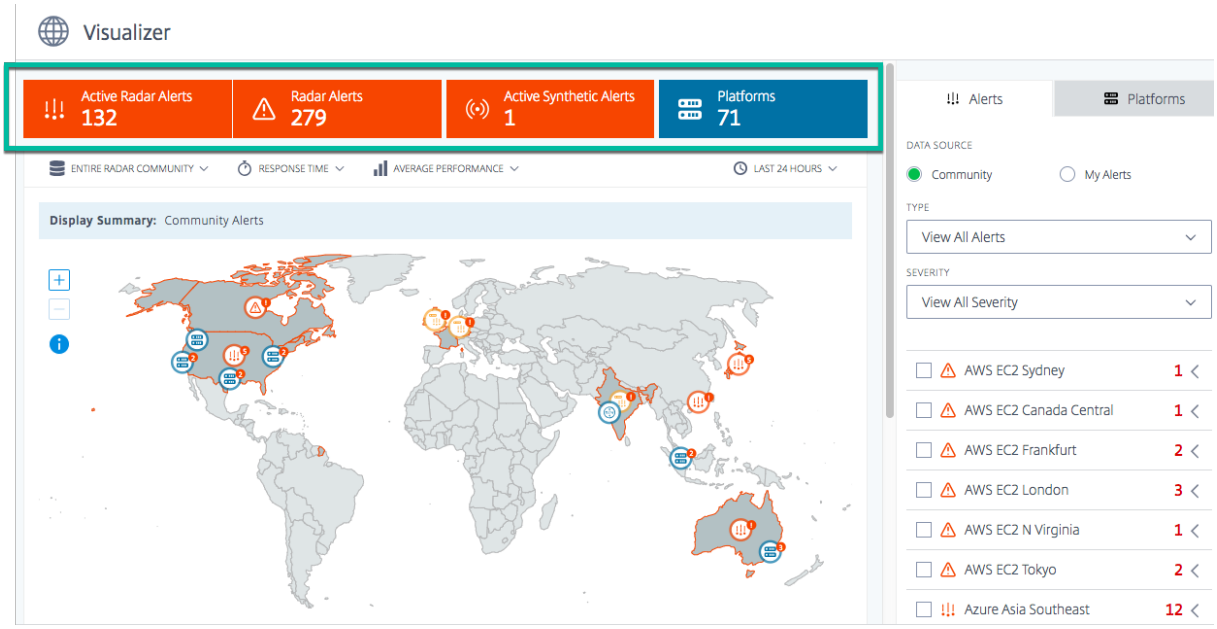
Las alertas de Radar Activo son actuales y en curso. De forma predeterminada, este mosaico muestra todas las alertas de las últimas 24 horas, pero cambia según el período de tiempo que seleccione el usuario.

Alertas sintéticas activas

Estas alertas se producen en tiempo real. Sonar, nuestro sistema de supervisión sintético que mide la disponibilidad global de un servicio o centro de datos, genera estas alertas.

Plataformas

El número de plataformas configuradas en la cuenta del cliente.



Opciones de visualización

Puede ver alertas y plataformas en el mapa utilizando los siguientes criterios:

Toda la comunidad de Radar o solo sus visitantes

Elija **Comunidad de Radar** para ver el rendimiento de las plataformas en toda la comunidad de Radar. O, alternativamente, para ver el rendimiento de sus visitantes a través de sus plataformas privadas, elija **Solo sus visitantes**.

Tiempo de respuesta o disponibilidad

Haga clic en cualquier plataforma del mapa o de la lista para ver su rendimiento según **disponibilidad** o **tiempo de respuesta**.

Mejor rendimiento o rendimiento promedio

Seleccione **Rendimiento promedio** o Mejor rendimiento para ver el rendimiento promedio/mejor que obtendría para sus plataformas.

El rendimiento promedio es similar a hacer un round robin entre sus plataformas y el **mejor rendimiento** es el rendimiento que obtenemos al usar ITM.

Cuando elige **Mejor rendimiento**, verá el rendimiento en el mapa basado en la plataforma de mejor rendimiento. Por ejemplo, si está mirando el rendimiento de un país específico y tiene dos plataformas seleccionadas, **Mejor rendimiento** colorea el mapa de país en función de la plataforma que tuvo el mejor rendimiento entre las dos (mayor disponibilidad o menor tiempo de respuesta) para ese país.

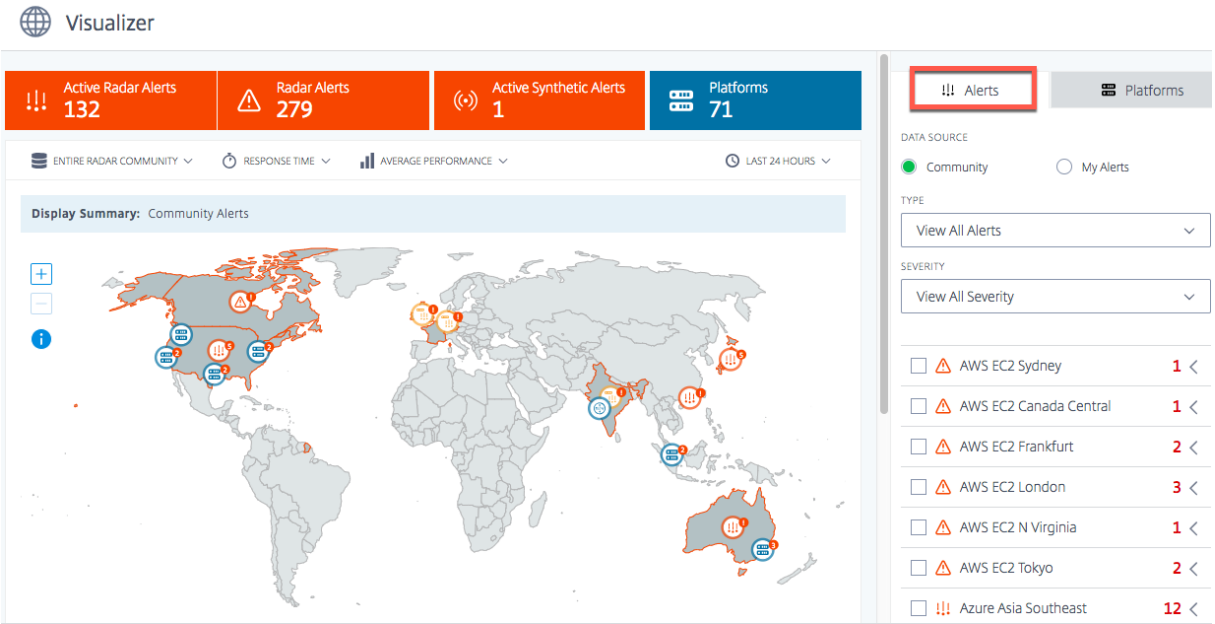
Alternativamente, si selecciona **Rendimiento medio**, verá el rendimiento en el mapa en función del promedio de todas las plataformas seleccionadas. Colorea el mapa del país con la disponibilidad promedio (o el tiempo de respuesta) de las dos plataformas.

Periodo de tiempo

Las alertas en el mapa se pueden generar con un periodo de tiempo de **últimos 60 minutos, últimas 24 horas, últimas 48 horas, últimos 7 días, últimos 30 días o un rango personalizado**. La vista predeterminada es las últimas 24 horas. Cada vez que cambia el período de tiempo, se actualizan los datos del mapa y se muestran las alertas activadas para ese período de tiempo.

Alertas

La ficha **Alertas** es la ficha predeterminada que se muestra al aterrizar en la página del visualizador. El origen de datos predeterminado que se muestra para un nuevo usuario sin alertas propias es **Comunidad.** Esto significa que todas las alertas que está viendo en el mapa como un nuevo usuario son alertas de comunidad. Aunque haya configurado alertas, pero no tenga alertas activas o continuas, la vista se establece de forma predeterminada como alertas de comunidad. Sin embargo, si configuró sus alertas y tiene alertas activas en curso, su vista predeterminada es la suya propia. Para obtener más información sobre las alertas, consulte Alertas.



Comunidad

Las alertas de la comunidad son problemas de rendimiento o anomalías observadas por ITM Radar que ocurren en toda la comunidad ITM. Estas alertas se miden a través de redes de usuarios finales de todo el mundo. Cuando abra el **visualizador** por primera vez como nuevo usuario, verá todas las alertas de la comunidad en el mapa. Una vez que haya configurado sus propias alertas, las verá en lugar de las alertas de la comunidad.

Sin embargo, si tiene plataformas privadas y alertas configuradas, verá sus propias alertas como **Mis alertas**, la vista predeterminada.

Mis alertas

Estas alertas son problemas de rendimiento o anomalías de sus plataformas privadas. Utiliza redes de usuarios finales en todo el mundo para medir estas alertas.

Como usuario nuevo, si no ve ninguna alerta, significa que no tiene ninguna alerta configurada. Puede ir a la página **Alertas** desde la barra lateral izquierda para configurar alertas para el rendimiento de sus plataformas. Pero primero tendrá que configurar sus plataformas privadas. Para configurar plataformas, puede ir a la página **Plataformas** desde la barra lateral izquierda o hacerlo sobre la marcha a través de la ficha **Plataformas**.

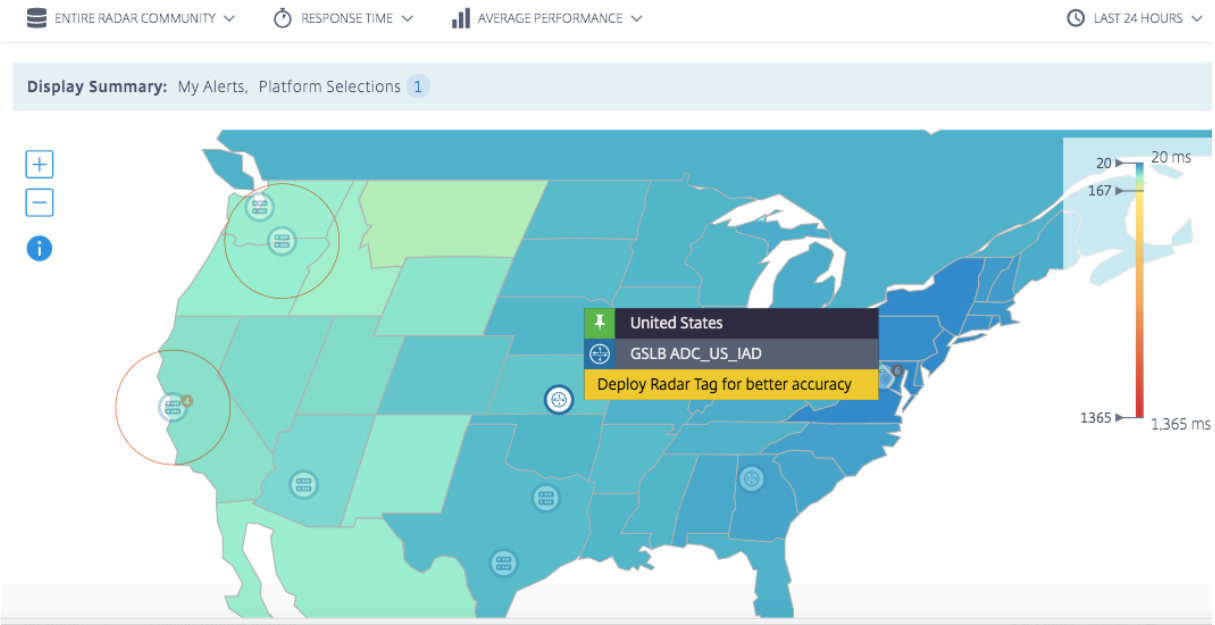
Detalles de la alerta

Puede pasar el cursor sobre la alerta en el mapa para ver el país y los servicios para los que se están activando las alertas. Para obtener más detalles sobre una alerta específica,

1. Haga clic en el icono de alerta en el mapa para marcar la casilla de la alerta de activación del servicio y resaltarla en la lista.
2. Haga clic en la flecha del lado derecho de la plataforma o servicio seleccionado para mostrar los detalles de la alerta, incluidos:

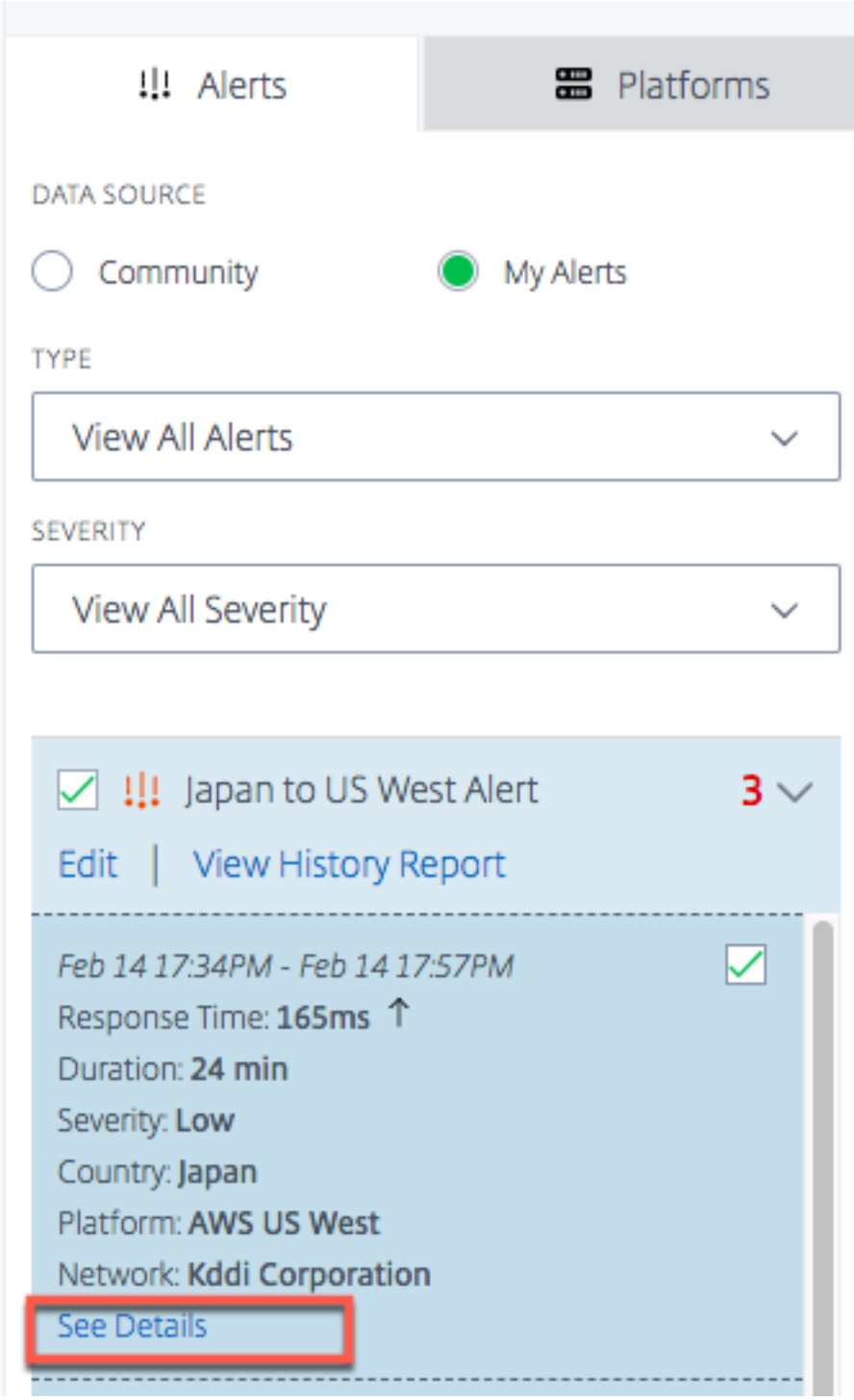
   a) **Disponibilidad** o **Tiempo de Respuesta** del origen de datos
   b) **Duración** de la alerta
   c) **Gravedad** de la alerta
   d) **País** de la red desde la que se miden los problemas
   e) Nombre de la **plataforma** para la que se activa la alerta.
   f) Nombre de la **red** desde la que se miden los problemas.

Alertas a**nivel estatal: alertas**activas con información sobre el rendimiento y la disponibilidad de nubes, centros de datos, CDN y otros servicios. Estas alertas se miden y se ven a nivel estatal dentro de los Estados Unidos.



Para profundizar en los detalles de la alerta, haga clic en **Ver detalles** para ir a la página **Alertas**.

> **NOTA:** Puede ver el enlace **Ver detalles** solo para sus propias alertas.

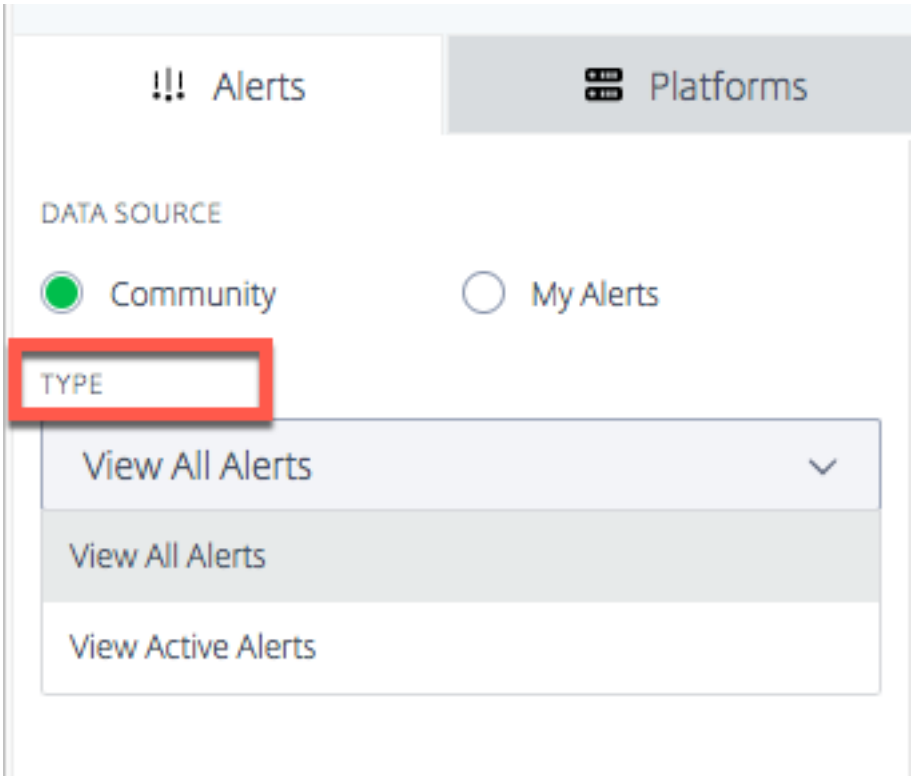


Tipo de alerta

El menú **Tipo** permite ver el siguiente tipo de alertas.

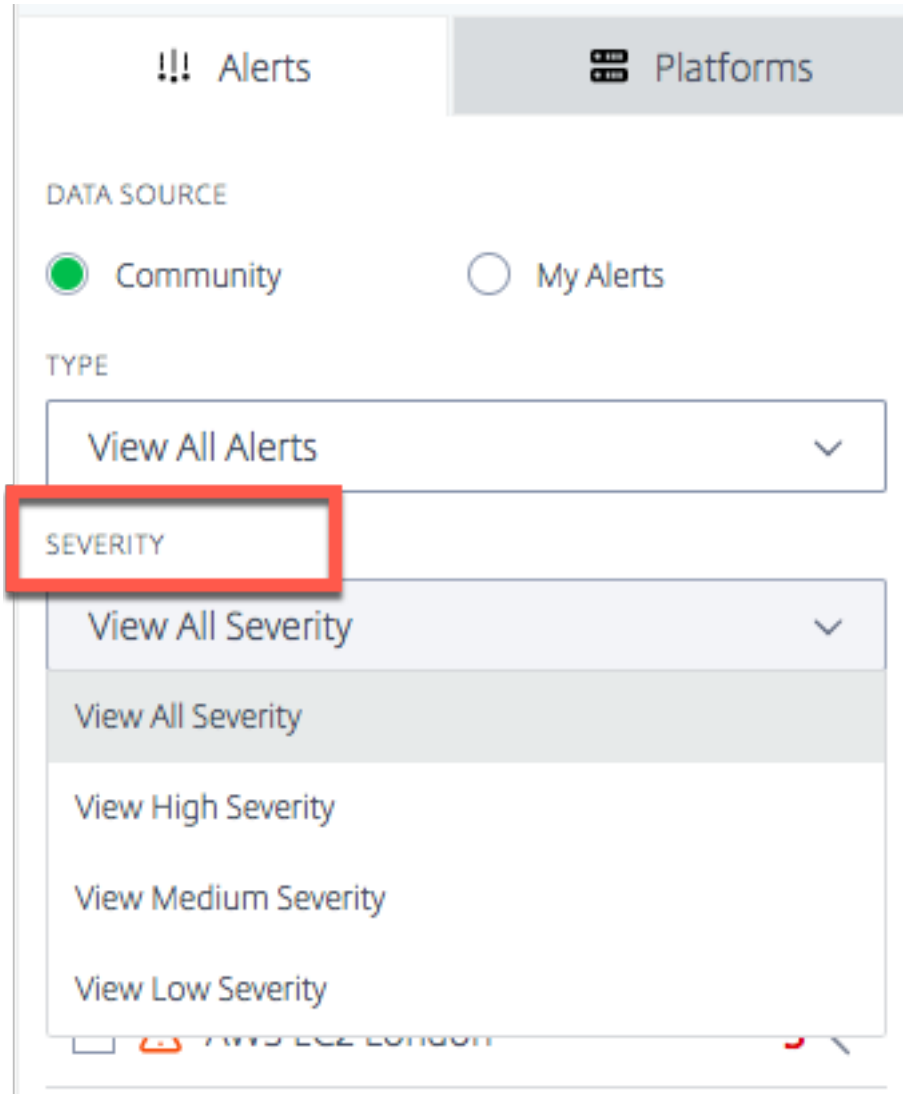
Todas las alertas Todas las alertas incluyen alertas activas e históricas. Las alertas históricas son alertas que se originaron posteriormente en el período de tiempo seleccionado.

Alertas activas Las alertas activas incluyen alertas que están en curso. Son válidos y actuales del período de tiempo especificado por el usuario.



Gravedad de alerta

Las alertas se pueden filtrar según la gravedad **alta, media** y **baja**. **Toda la gravedad** es la visualización predeterminada.



Lógica de gravedad Para disponibilidad:

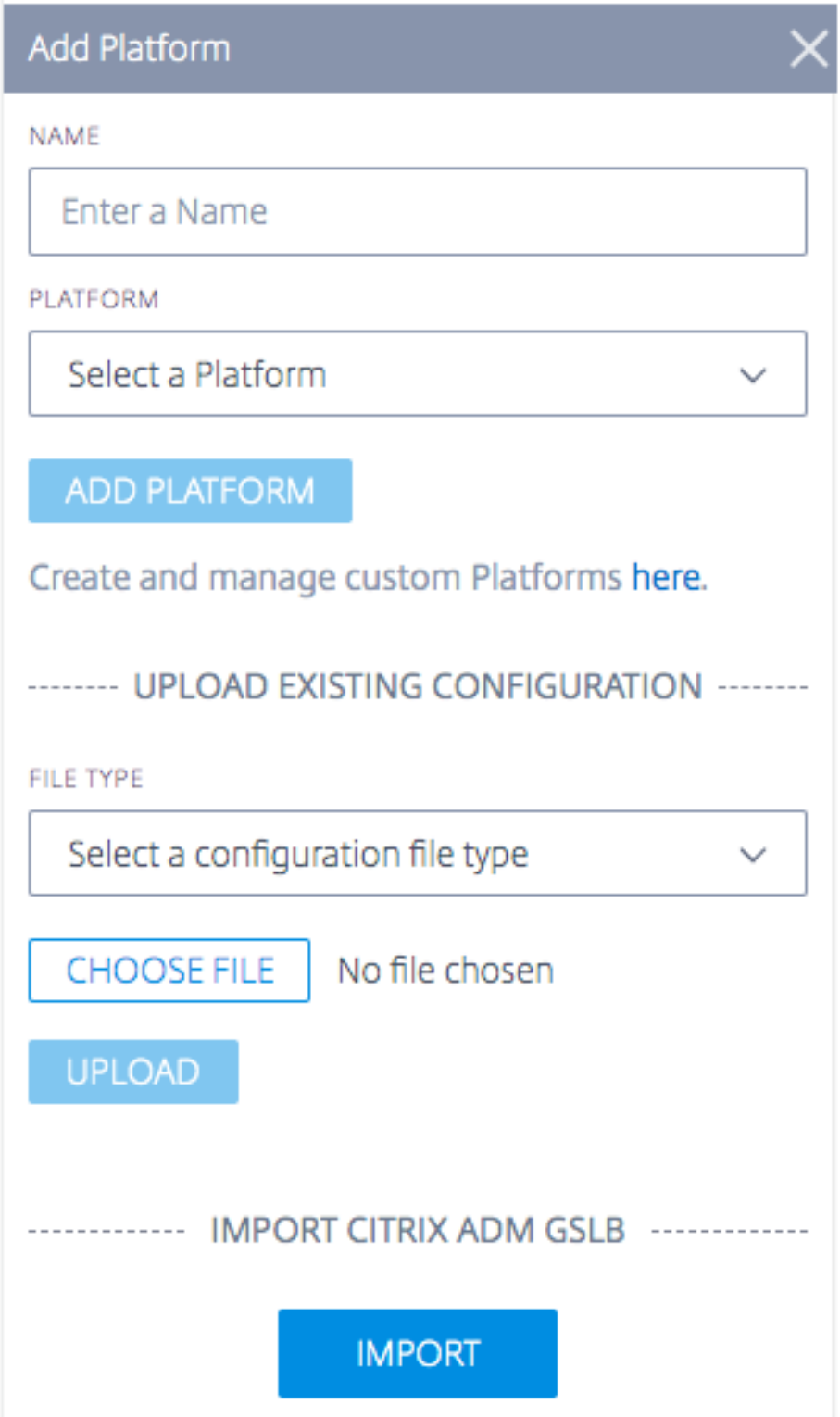
- Si más del 50% por debajo del umbral -> Gravedad es **alta**
- Si más del 25% pero menos del 50% por debajo del umbral -> Gravedad es **Media**
- Si menos del 25% por debajo del umbral -> Gravedad es **Baja**

Tiempo de respuesta:

- Si más de 200% sobre el umbral -> Gravedad es **alta**
- Si más del 100% supera el umbral pero menos del 200% -> Gravedad es **Media**
- Si menos del 100% sobre el umbral -> Gravedad es **baja**

Plataformas

Al seleccionar la ficha **Plataformas**, verá la lista de las plataformas que agregó. Sin embargo, si es un usuario nuevo y aún no ha configurado ninguna plataforma, puede agregar una plataforma comunitaria aquí sobre la marcha o configurar una plataforma privada haciendo clic en el enlace **Crear y administrar plataformas personalizadas aquí**.



Agregar una plataforma comunitaria

1. Para agregar una plataforma de comunidad, haga clic en el icono + situado junto a la barra **Agregar plataforma**.
2. Asigne un nombre a la plataforma y seleccione la plataforma de la lista de plataformas de la comunidad en el menú **Plataforma**.
3. Haga clic en **Agregar plataforma**.

Agregar una plataforma personalizada o privada

1. Para agregar una plataforma privada, haga clic en el icono + situado junto a la barra **Agregar plataforma**.
2. Haga clic en el enlace **Crear y gestionar plataformas personalizadas aquí**, que le lleva a la página **Plataformas**, donde puede agregar una nueva plataforma privada. Alternativamente, puede ir a la página **Plataformas** desde la barra lateral izquierda.

Cargar configuración existente: NetScaler y F5 BIG-IP DNS

Esta opción le permite elegir un archivo de configuración DNS NetScaler o F5 BIG-IP e importar la configuración (de sus plataformas existentes) directamente. Crea automáticamente plataformas privadas para la configuración de DNS de NetScaler o F5 BIG-IP.

Importar Citrix GSLB desde el servicio ADM

Esta opción le permite importar directamente todas las GSLB configuradas en el servicio ADM.

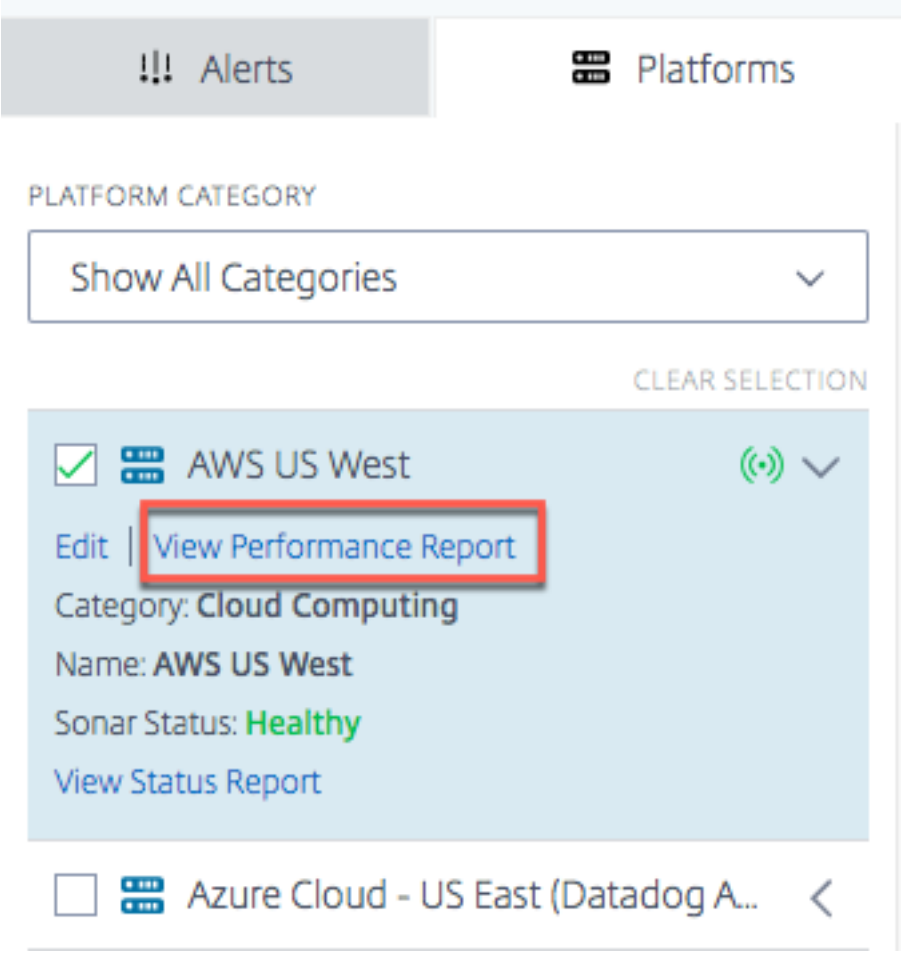
Si utiliza Citrix Cloud ADM Service, puede importar las GSLB configuradas allí. La información básica del sitio (IP y nombre) se importan como plataformas ITM. ITM geolocaliza el sitio y permite que la plataforma se muestre en el visualizador para el análisis del rendimiento.

Informe de rendimiento

El Informe de rendimiento del radar proporciona detalles sobre plataformas específicas, alertas activadas y cada red desde la que se midió. El informe muestra las mediciones de tiempo de respuesta o disponibilidad y el período de tiempo del problema que se midió. Incluye todos los filtros que se aplicaron en el **visualizador**.

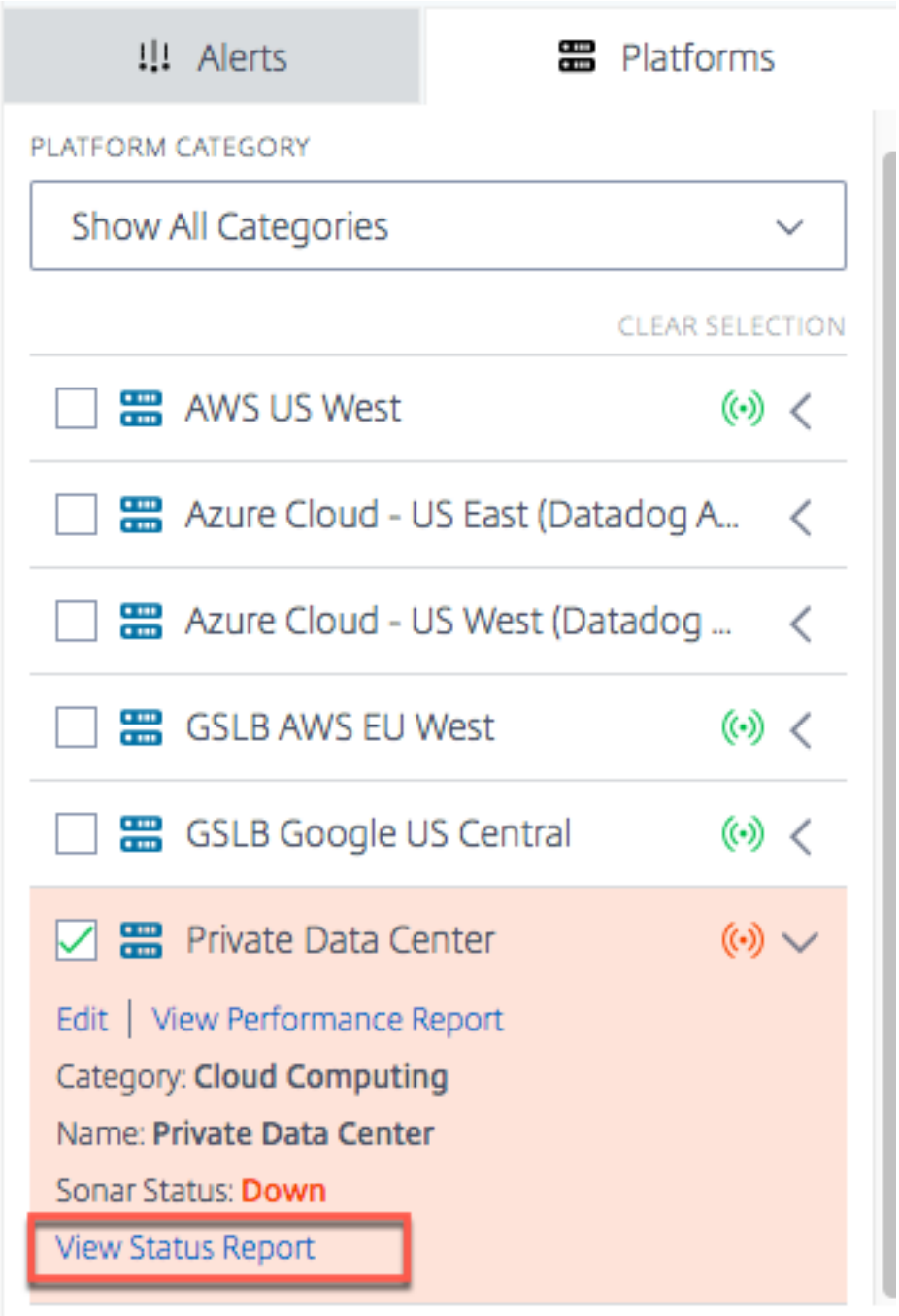
Para ver los detalles de rendimiento de una plataforma específica para la que se activó la alerta, haga lo siguiente.

1. Haga clic en el icono de la plataforma o en el icono de alerta del mapa para resaltarlo y marque la casilla de la lista de la derecha.
2. Haga clic en la flecha situada junto a la plataforma o alerta para expandirla.
3. Haga clic en el enlace **Ver informe de rendimiento** para ir a la página **Informe de rendimiento del** radar.

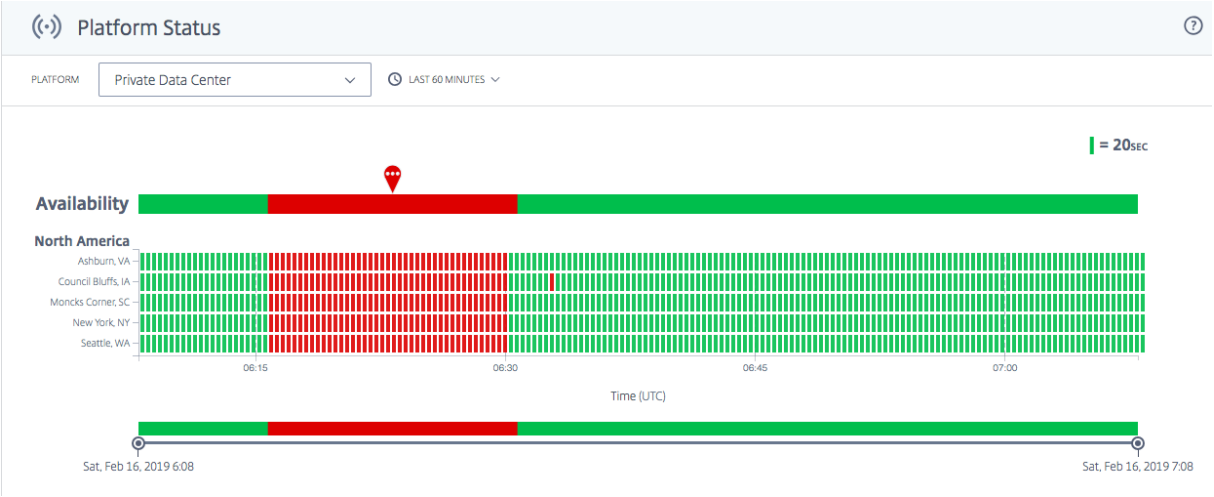


Informe de estado

Para las alertas de supervisión sintética, puede ver los detalles de las alertas expandiendo la plataforma para ver los detalles y, a continuación, haciendo clic en **Ver informe de estado**.



El enlace **Ver informe de estado** le lleva a la página **Estado de la plataforma** Sonar y le proporciona detalles del estado de su plataforma basándose en comprobaciones de supervisión sintética en tiempo real.



Radar

September 13, 2023

Introducción

El Radar forma la columna vertebral de la metodología de recopilación de datos. Radar utiliza un script JavaScript incrustado en una página de contenido o páginas del proveedor de aplicaciones para recopilar información sobre el rendimiento y la disponibilidad de un centro de datos o una plataforma de entrega.

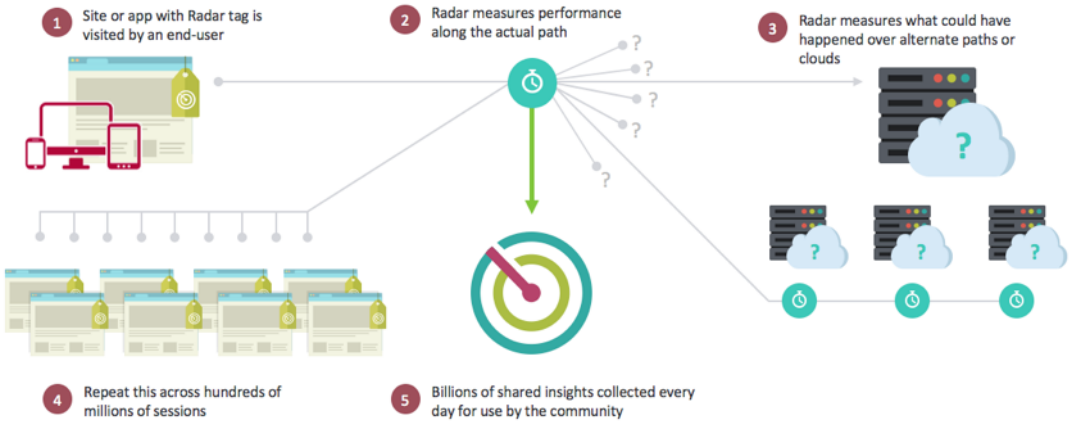
El cliente Radar es una aplicación JavaScript que se ejecuta en páginas web del cliente y dentro de aplicaciones móviles. Su objetivo principal es recopilar los datos de rendimiento de la red que se utilizan para tomar decisiones de enrutamiento inteligentes a través de Openmix y proporcionar complementos opcionales para habilitar otros servicios de administración inteligente del tráfico de NetScaler, como el tiempo de carga de la página, la temporización de los recursos de la página y las métricas de reproducción de vídeo.

El cliente Radar tiene todas las funciones, pero ligero y discreto. El cliente espera hasta que la mayoría de los recursos de la página se hayan descargado antes de realizar la mayor parte de su trabajo, y toda la comunicación de red se realiza de manera asíncrona siempre que sea posible. Estas instrucciones especifican qué plataforma medir a continuación durante la sesión, escogida entre las plataformas de la comunidad y cualquier plataforma privada específica para ese miembro de la comunidad. También indican los tipos de mediciones que se van a realizar, que pueden incluir disponibilidad, tiempo de ida y vuelta, rendimiento u otra recopilación de métricas.

Para que sea lo más pequeño posible, el JavaScript se compila con optimizaciones avanzadas utilizando el compilador de cierre de Google. Las funciones opcionales avanzadas se entregan como complementos para los clientes que opten por utilizarlas.

Comunidad de Radar

Utilizando un enfoque único basado en la comunidad, Radar aporta una transparencia sin igual al rendimiento global y la disponibilidad de las infraestructuras públicas más grandes del mundo, desde Cloud Computing y Almacenamiento hasta Redes de Entrega de Contenido y Aplicaciones. Con Radar, los clientes pueden encontrar rápidamente las plataformas de mejor rendimiento y peor rendimiento para cada uno de sus visitantes.



Radar es la primera cooperativa de supervisión en la nube de Internet. Convertirse en miembro de la Comunidad significa acceso ilimitado a nuestra base de datos de informes históricos, incluida la segmentación detallada por proveedor, país y red.

Ser miembro de la comunidad de Radar también proporciona un amplio conjunto de herramientas para capturar los niveles de servicio proporcionados por las infraestructuras de entrega de contenido internas y externas. Exclusiva de Radar es la capacidad de utilizar a los visitantes de su sitio web para medir la experiencia que recibirían de plataformas que no utilizan actualmente una empresa. La misma metodología permite realizar evaluaciones objetivas de las plataformas en la nube a lo largo de su ciclo de vida, incluida la evaluación continua del rendimiento en relación con los acuerdos de nivel de servicio.

Al agregar una etiqueta JavaScript simple a su página web o un SDK a aplicaciones móviles, los clientes pueden convertir a cada uno de sus visitantes en un 'agente de prueba' virtual. El Radar desencadena mediciones basadas en dispositivos descargando objetos de referencia y comparando la infraestructura interna y externa, los centros de datos, las redes de entrega y las plataformas en la nube según lo ven los usuarios finales reales de sitios o aplicaciones web.

Beneficios clave de la participación

Radar aborda múltiples desafíos de la entrega web a través de su enfoque de supervisión y recolección de datos. Los principales beneficios de participar en la comunidad de Radar son:

- Entorno de pruebas masivo, con usuarios finales en cada red en cada ubicación (más de 42 000 redes reconocidas hasta el momento).
- Obtenga información importante sobre los proveedores de servicios antes de la prueba para tomar una decisión más informada.
- Transparencia en el rendimiento de los proveedores actuales y cómo se comportan en las geografías donde usted tiene y no tiene usuarios.
- Centrarse en las métricas que marcan una diferencia real para los usuarios web y móviles (Rendimiento, Disponibilidad y QoS).
- Visión global (más de 190 países) sin restricciones de la información hasta los niveles de país, red, región y estado.
- Datos reales e imparciales mediante el uso de usuarios finales Los datos de radar son información del «mundo real» y no una prueba sintética o una mejor suposición.
- Todos los usuarios no son iguales: Entender diferentes máquinas, conexiones y dispositivos.
- Visibilidad del rendimiento de las páginas reales.

Puntos de referencia

ITM Radar ofrece 3 puntos de referencia principales:

- Evaluación comparativa de la comunidad
- Benchmarking privado
- Evaluación comparativa de carga de página

Evaluación comparativa de la comunidad de CDN, Cloud y Data Centers

Las mediciones de la comunidad se obtienen a través de un modelo de aprovisionamiento multitudinario que proporciona al cliente una visión del rendimiento y la disponibilidad de un proveedor a nivel geográfico y lógico a nivel global. Las mediciones de la comunidad permiten realizar comparaciones entre la calidad de la experiencia de un proveedor vista por el usuario final y permiten un análisis hipotético al evaluar a los vendedores y proveedores para la distribución de contenido y aplicaciones. Al utilizar un modelo de crowdsourcing, los clientes de ITM se benefician al obtener un mayor nivel de granularidad y calidad de los datos en la evaluación y supervisión del rendimiento de los proveedores, incluso en lugares donde un cliente puede no tener una alta densidad de usuarios, o incluso cualquier usuario en absoluto.

Las mediciones en sí mismas utilizan un conjunto estándar de objetos ubicados en los diferentes proveedores de Cloud y CDN que los usuarios finales descargan cuando ejecutan el cliente JavaScript de Radar, o la lógica de SDK móvil, en el sitio o aplicación de un propietario de contenido.

Las siguientes métricas se notifican a ITM y se presentan en las interfaces de informes de Portal o API:

- Availability: si el objeto se carga o no.
- Tiempo de respuesta: cuánto tiempo tarda el servidor en responder a una solicitud posterior, una vez completado todo el ruido de establecer una conexión. Esto es una aproximación relativamente cercana del tiempo de ida y vuelta (RTT) de TCP desde el navegador hasta el proveedor.
- Throughput: es la velocidad de datos de la conexión, en kilobits por segundo, medida a partir de la recuperación de un objeto de 100 KB.

Benchmarking privado

Como parte del despliegue de Radar Tag, ITM ofrece al cliente la posibilidad de crear sus propias pruebas «de referencia» que miden los visitantes del cliente. Esto puede ser para Data Centers o sus propios contratos CDN y Cloud. Al igual que con las mediciones de referencia de la comunidad, se proporcionan las mismas métricas: Disponibilidad, Tiempo de Respuesta y Rendimiento, lo que permite al cliente evaluar eficazmente una estrategia de entrega de contenido existente.

Esta información privada solo está disponible para el cliente y no se comparte.Entre los usos de ejemplo se incluyen:

- Arquitectura de centros de datos propios
- Usando su propio objeto de prueba o página
- Utilizar su propio contrato y cuenta con un proveedor específico o conjunto de proveedores

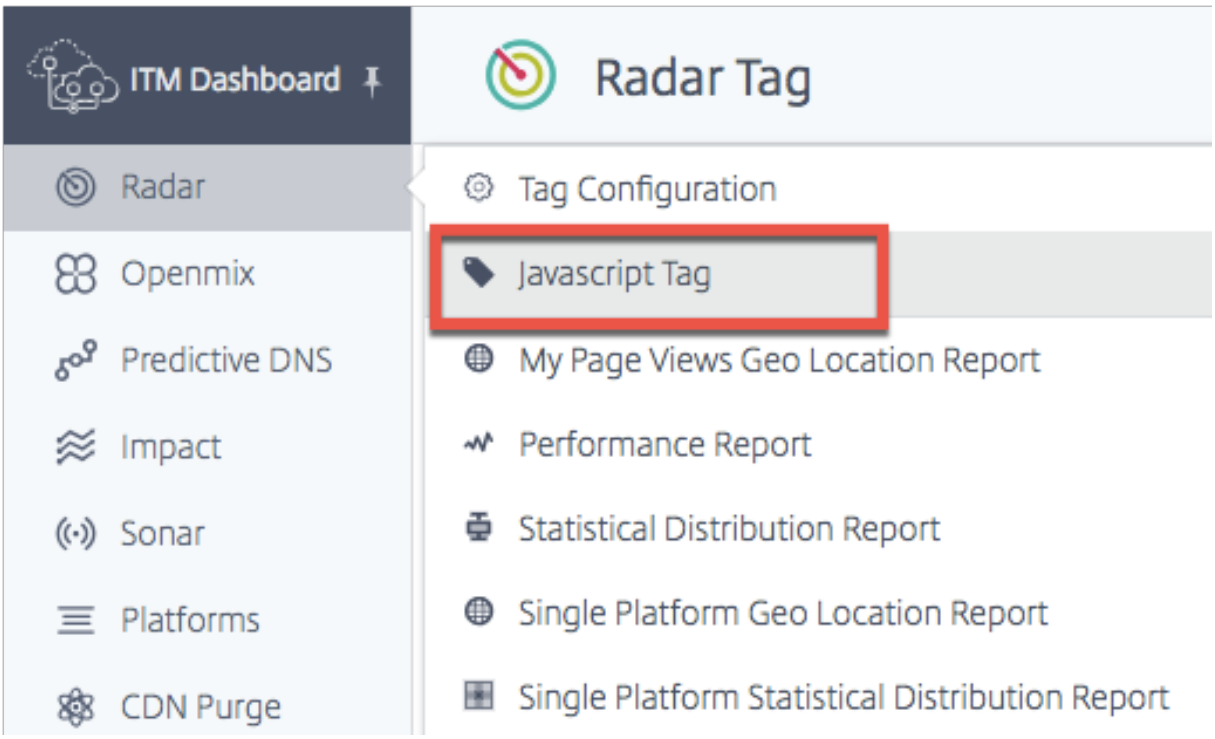
Evaluación comparativa de carga de páginas de Radar

Dentro de Radar ITM ofrece la posibilidad de que el cliente vea información detallada sobre cómo se descargan las páginas en las que se implementa la etiqueta. ITM proporciona información que le permite ver el rendimiento real de los usuarios finales al interactuar con sus páginas web. Los datos se proporcionan a través de la API de sincronización de navegación compatible con muchos de los exploradores de versiones más recientes.

Etiqueta de Radar

La etiqueta Radar se puede integrar mediante un fragmento de JavaScript. Para navegar a la página **Etiqueta de Radar**, haga lo siguiente:

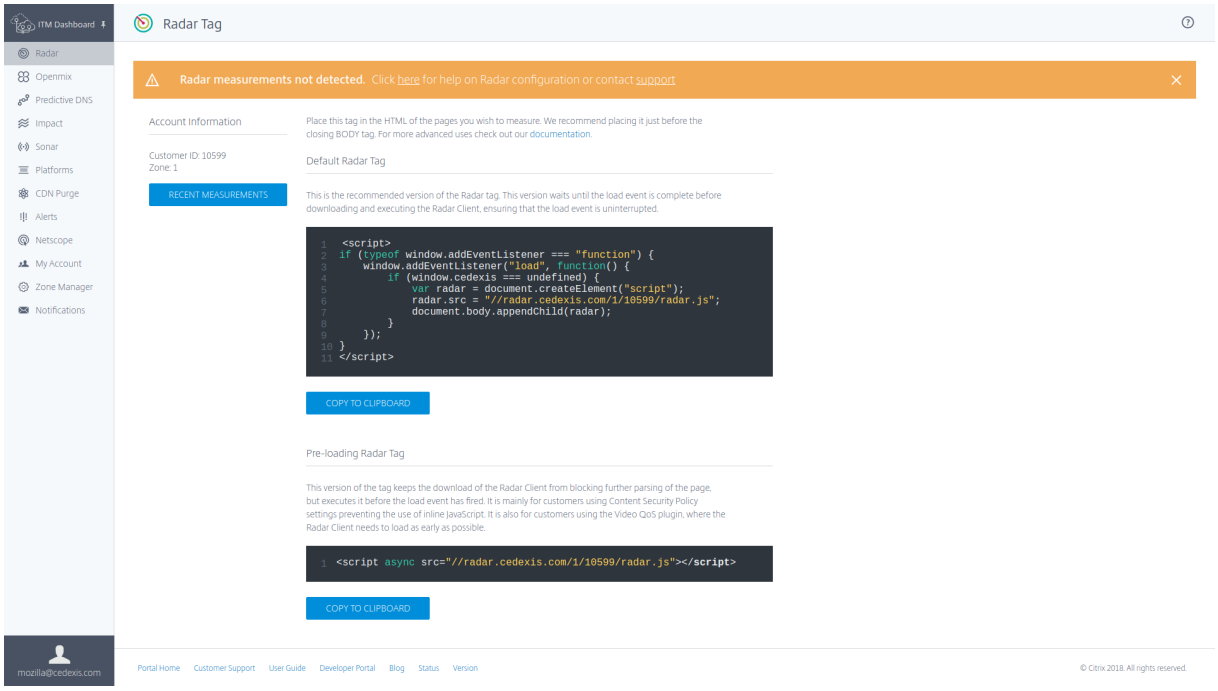
1. Inicie sesión en el portal de administración inteligente del tráfico de NetScaler.
2. En el menú de navegación de la izquierda, seleccione **Radar > Javascript Tag**.



Se abrirá la página **Etiqueta de Radar**.

Si aún no ha configurado la etiqueta de Radar, verá una barra horizontal naranja en la parte superior de la pantalla que le indica que no se han detectado mediciones de Radar.

Esta barra naranja también aparecerá si la etiqueta no se ha configurado correctamente.



Alternativamente, si la etiqueta de Radar funciona como se esperaba, verá una barra horizontal verde que le indica que las mediciones de Radar se obtuvieron correctamente.

En esta página puede seleccionar la versión de etiqueta que sea aplicable a su uso y copiarla en el portapapeles.

Nota: Es importante no cambiar este fragmento de JavaScript. El código incluye información importante que, si se cambia, puede crear un comportamiento inesperado o poco confiable.

Integración de la etiqueta de Radar

Integrar la etiqueta Radar es relativamente simple. Todo lo que necesita hacer es agregar uno de los fragmentos de JavaScript a continuación al marcado de su sitio. Colóquelo en el HTML de las páginas que desee medir. Recomendamos colocarlo en la parte inferior de la página antes de la etiqueta del cuerpo de cierre`</body>`.

Etiqueta de Radar predeterminada

Esta es la versión recomendada de la etiqueta Radar. Esta versión espera hasta que se complete el evento de carga antes de descargar y ejecutar el cliente de Radar, asegurando que el evento de carga no se interrumpa.

```
<script>
if (typeof window.addEventListener === "function") {

```



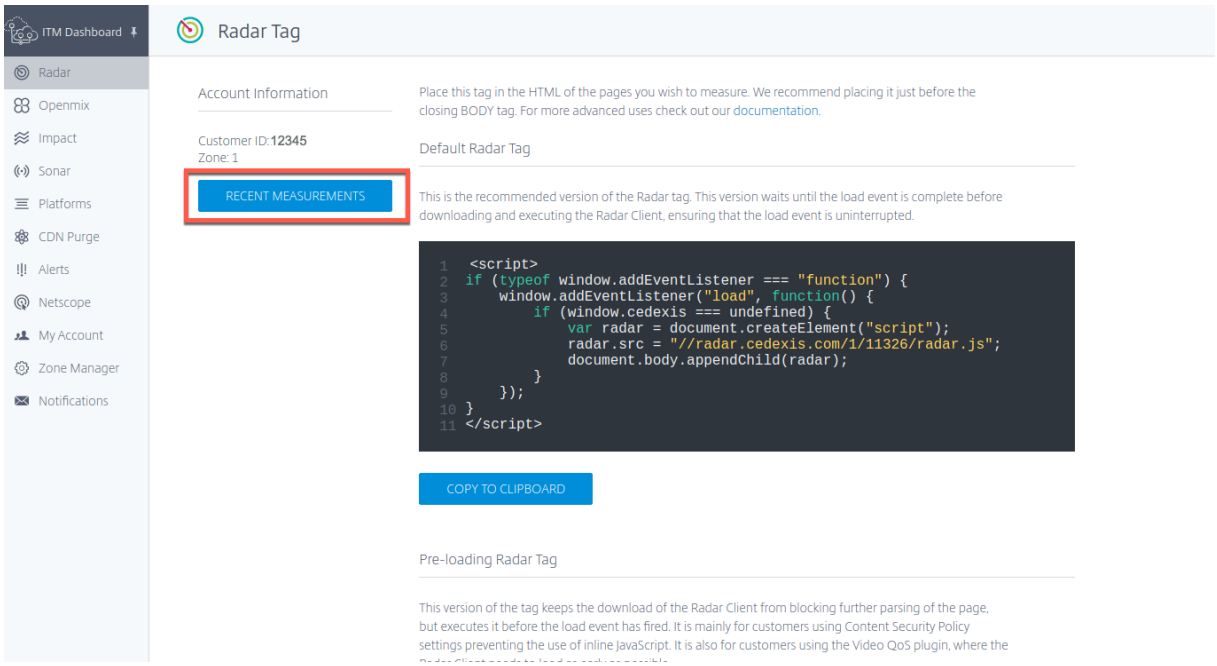
```
4       window.addEventListener("load", function() {
5
6           if (window.cedexis === undefined) {
7
8               var radar = document.createElement("script");
9               radar.src = "//radar.cedexis.com/1/54621/radar.js"; //
                    replace with user specific value
10              document.body.appendChild(radar);
11           }
12
13       }
14   );
15   }
16
17 </script>
18 <!--NeedCopy-->
```

Esta versión de la etiqueta evita que la descarga del cliente de Radar bloquee el análisis de la página, pero la ejecuta antes de que se desencadene el evento de carga. Es principalmente para los clientes que utilizan la configuración de la directiva de seguridad de contenido que impide el uso de JavaScript en línea. También es para los clientes que utilizan el complemento Video QoS, donde el cliente Radar debe cargarse lo antes posible.

```
1 <script src="//radar.cedexis.com/1/54621/radar.js" async></script>
2 <!--NeedCopy-->
```

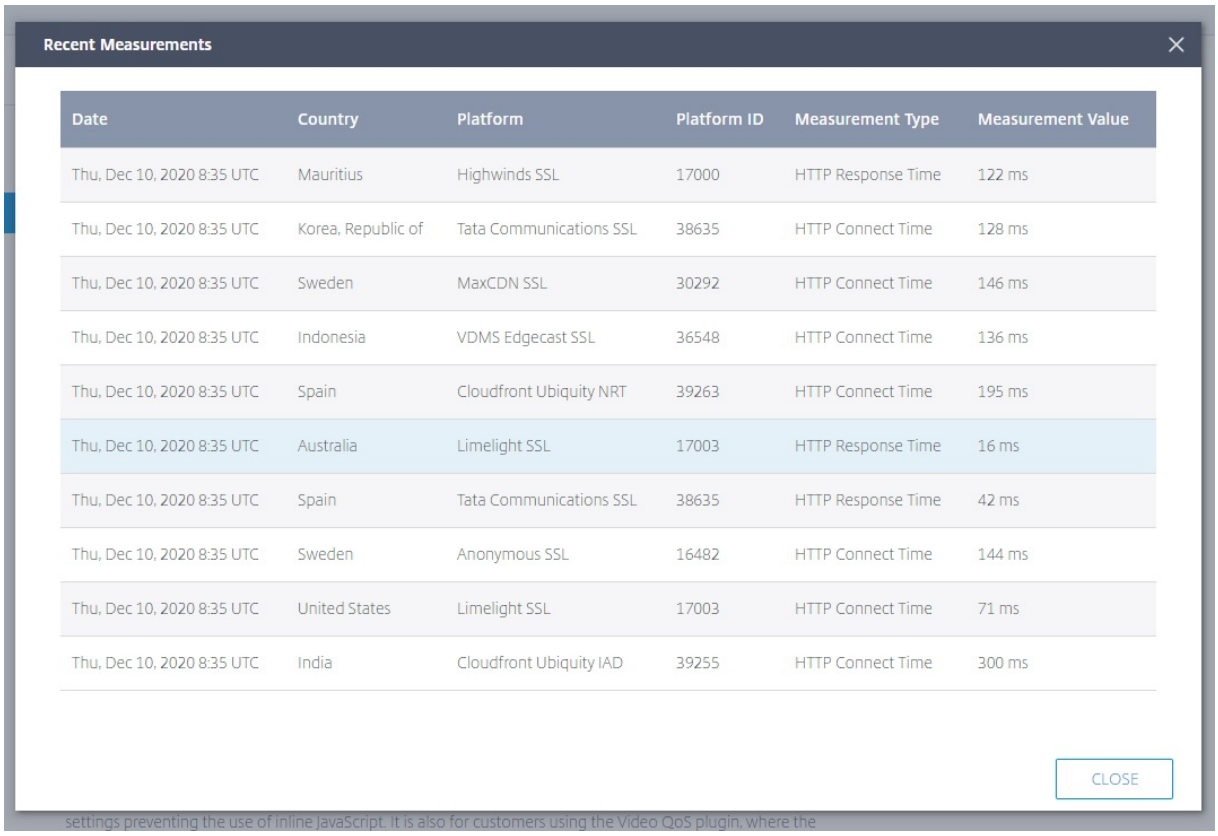
Medidas recientes

La tabla **Medidas recientes** le permite ver las últimas mediciones realizadas con Radar.



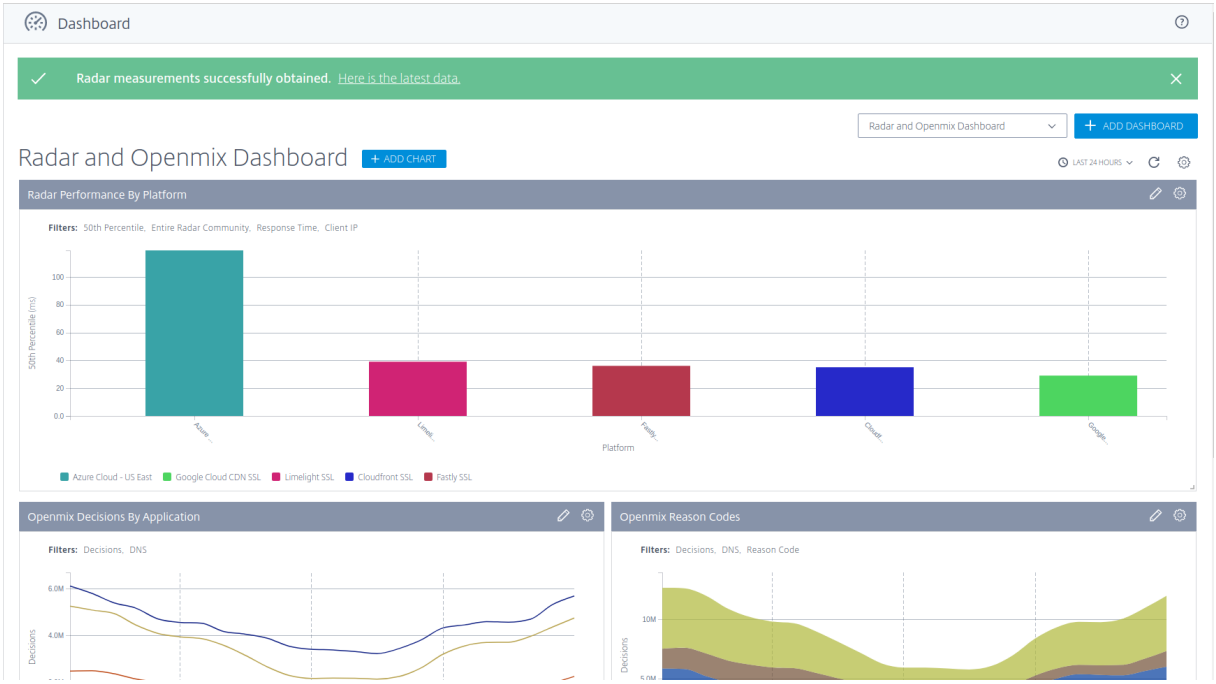
Haga clic en el botón **Medidas recientes**. Le da la siguiente información:

- Fecha y hora en que se tomó la medición en UTC.
- País en el que se realizó la medición.
- La plataforma que se utilizó para tomar la medición.
- El ID de la plataforma.
- El tipo de medida tomada es decir, Tiempo de conexión (en milisegundos), Tiempo de respuesta (en milisegundos) o Rendimiento (en kilobits por segundo)
- El valor real de la medición en milisegundos (para el tiempo de conexión y el tiempo de respuesta) o Kilobits por segundo (para el rendimiento).



Date	Country	Platform	Platform ID	Measurement Type	Measurement Value
Thu, Dec 10, 2020 8:35 UTC	Mauritius	Highwinds SSL	17000	HTTP Response Time	122 ms
Thu, Dec 10, 2020 8:35 UTC	Korea, Republic of	Tata Communications SSL	38635	HTTP Connect Time	128 ms
Thu, Dec 10, 2020 8:35 UTC	Sweden	MaxCDN SSL	30292	HTTP Connect Time	146 ms
Thu, Dec 10, 2020 8:35 UTC	Indonesia	VDMS Edgecast SSL	36548	HTTP Connect Time	136 ms
Thu, Dec 10, 2020 8:35 UTC	Spain	Cloudfront Ubiquity NRT	39263	HTTP Connect Time	195 ms
Thu, Dec 10, 2020 8:35 UTC	Australia	Limelight SSL	17003	HTTP Response Time	16 ms
Thu, Dec 10, 2020 8:35 UTC	Spain	Tata Communications SSL	38635	HTTP Response Time	42 ms
Thu, Dec 10, 2020 8:35 UTC	Sweden	Anonymous SSL	16482	HTTP Connect Time	144 ms
Thu, Dec 10, 2020 8:35 UTC	United States	Limelight SSL	17003	HTTP Connect Time	71 ms
Thu, Dec 10, 2020 8:35 UTC	India	Cloudfront Ubiquity IAD	39255	HTTP Connect Time	300 ms

La barra de mediciones de Radar también aparecerá en la página del **Panel** de control de Radar cuando inicie sesión por primera vez en el portal ITM.



Integración con aplicaciones móviles

La integración con aplicaciones móviles se lleva a cabo a través de envoltorios alrededor de vistas web ocultas que ejecutan el cliente JavaScript. Esto garantiza que los datos recopilados en exploradores y aplicaciones móviles sean coherentes.

Instrucciones para integrar Radar con la aplicación iOS

Este siguiente repositorio de GitHub contiene el código contenedor e instrucciones paso a paso para integrar Radar con la aplicación iOS:

Radar Runner para iOS

Instrucciones para integrar Radar con Android

Android Radar es una biblioteca cliente que facilita la integración de Radar en aplicaciones Android. Se puede encontrar aquí:

Biblioteca AndroidRadar

Integración con NetScaler

La etiqueta Radar es importante porque proporciona a Openmix mediciones que permiten a Openmix tomar mejores decisiones de enrutamiento. Cuantas más páginas web usen la etiqueta, mejores son las decisiones de enrutamiento.

Los métodos siguientes le permiten colocar la etiqueta JavaScript de Radar en su página web mediante NetScaler. Puede utilizar la línea de comandos o la Utilidad de configuración de NetScaler.

Estos métodos le permiten inyectar la etiqueta Radar en sus respuestas. Para inyectar la etiqueta Radar, debe usar reescrituras. Las reescrituras se dividen en tres pasos: crear acciones, configurar directivas y directivas de enlace.

Configuración de la línea de comandos

Línea de comandos Configuración de la acción de reescritura Plantilla:

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-pattern <expression> | -search <expression>] [-refineSearch <string>] [-comment <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add rewrite action radar_tag action insert_after HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).BEFORE_STR("</body>") '"<script async src=\\"//radar.cedexis.com/1/<customer_id>/radar.js\\"></script>"'
<!--NeedCopy-->
```

Nota: Inserte su propio ID de cliente donde dice`<customer_id>`

Línea de comandos configurar la directiva de reescritura Plantilla:

```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <string>] [-logAction <string>]
<!--NeedCopy-->
```

Ejemplo:

```
add rewrite policy radar_tag_policy HTTP.RES.HEADER("Content-Type").TO_LOWER.CONTAINS("text/html") radar_tag_action
<!--NeedCopy-->
```

Directiva de reescritura de enlace de línea de comandos Plantilla 1:

```
bind vpn vserver <name> [-policy <string> [-priority <positive_integer>] [-secondary] [-groupExtraction] [-gotoPriorityExpression <expression>] [-type <type>]] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask> ] [-staServer <URL> [-staAddressType ( IPV4 | IPV6 )]] [-appController <URL>] [-sharefile <string>]
<!--NeedCopy-->
```

Ejemplo 1:

```
bind vpn vserver <name_of_vserver> -policy radar_tag_policy -type RESPONSE -priority 10
```



```
<!--NeedCopy-->
```

Plantilla 2:

```
bind cs vserver <name> (-lbvserver <string> | -vServer <string> | (-
    policyName <string> [-targetLBVserver <string>] [-priority <
    positive_integer>] [-gotoPriorityExpression <expression>] [-type (
    REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>) ] ) | (-
    domainName <string> [-TTL <secs>] [-backupIP <ip_addr|ipv6_addr|*>]
    [-cookieDomain <string>] [-cookieTimeout <mins>] [-sitedomainTTL <
    secs>]))
<!--NeedCopy-->
```

Ejemplo 2:

```
bind cs vserver <name_of_vserver> -policyName radar_tag_policy -type
    RESPONSE -priority 10
<!--NeedCopy-->
```

Plantilla 3:

```
bind lb vserver <name>@ (<serviceName>@ [- weight <positive_integer>])
    | <serviceGroupName>@ | (- policyName <string>@ [-priority <
    positive_integer>] [- gotoPriorityExpression <expression>] [-type (
    REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>) ] )
<!--NeedCopy-->
```

Ejemplo 3:

```
bind lb vserver <name_of_vserver> -policyName radar_tag_policy -type
    RESPONSE -priority 10
<!--NeedCopy-->
```

Plantilla 4:

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression>]
    [-type <type>] [-invoke (<labelType> <labelName>) ]
<!--NeedCopy-->
```

Ejemplo 4:

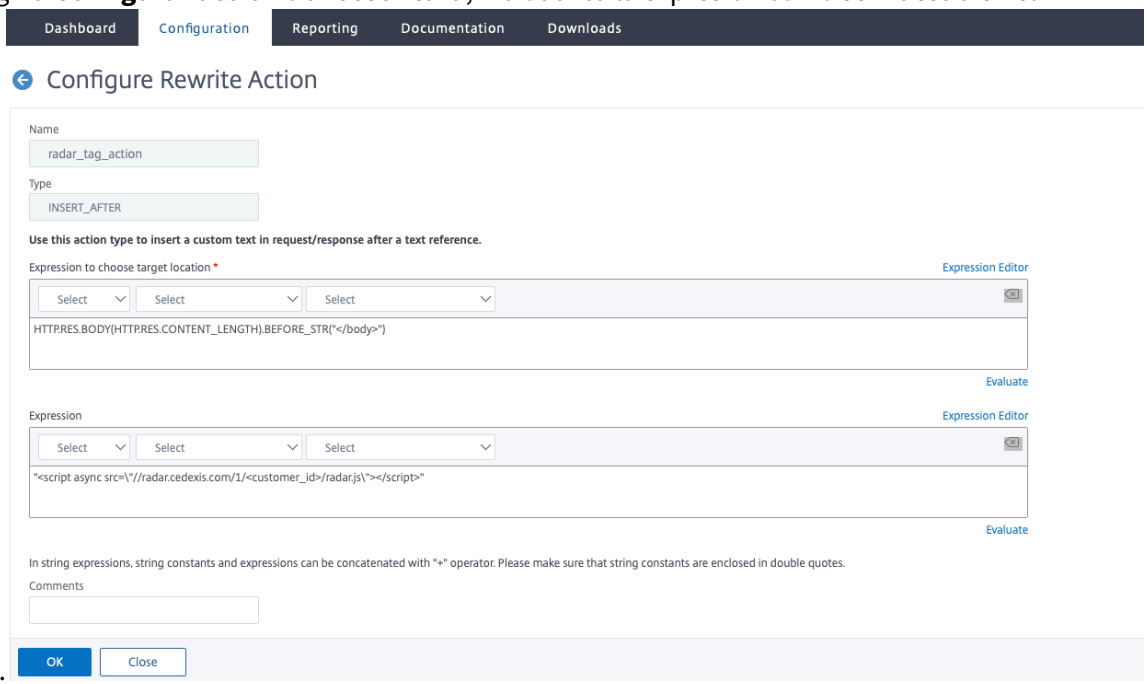
```
bind rewrite global radar_tag_policy 100 -type RES_DEFAULT
<!--NeedCopy-->
```

Configuración de la utilidad GUI

Acción de reescritura de GUI

1. En el menú de navegación de la izquierda de la página **Configuración de NetScaler**, vaya a **AppExpert** -> **Rewrite -> Rewrite** -> **Rewrite Actions**

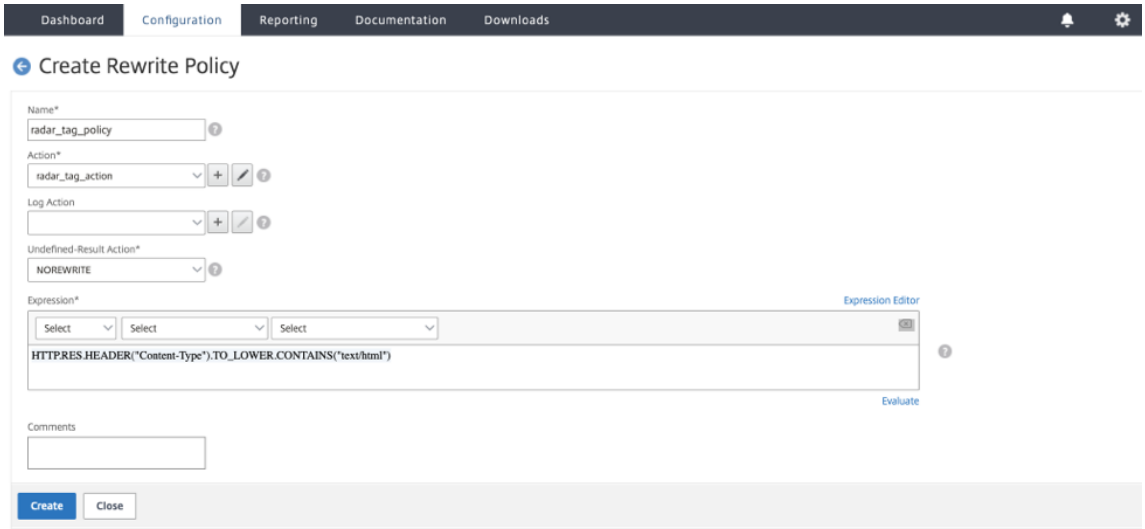
2. Seleccione el botón **Agregar**.
3. En la página **Configurar acción de reescritura**, introduzca la expresión como se muestra en el ejemplo.



4. En el script de Radar, introduzca su ID de cliente en el espacio marcado`<customer_id>`.
5. Seleccione **OK**. Ha completado la creación de la acción de reescritura.

Directiva de reescritura de GUI

1. En el menú de navegación de la izquierda de la página **Configuración de NetScaler**, vaya a **AppExpert** -> **Rewrite -> Rewrite** -> **Rewrite Policies**
2. Seleccione el botón **Agregar**.
3. En la página **Configurar directiva de reescritura**, introduzca la expresión como se muestra en el ejemplo.

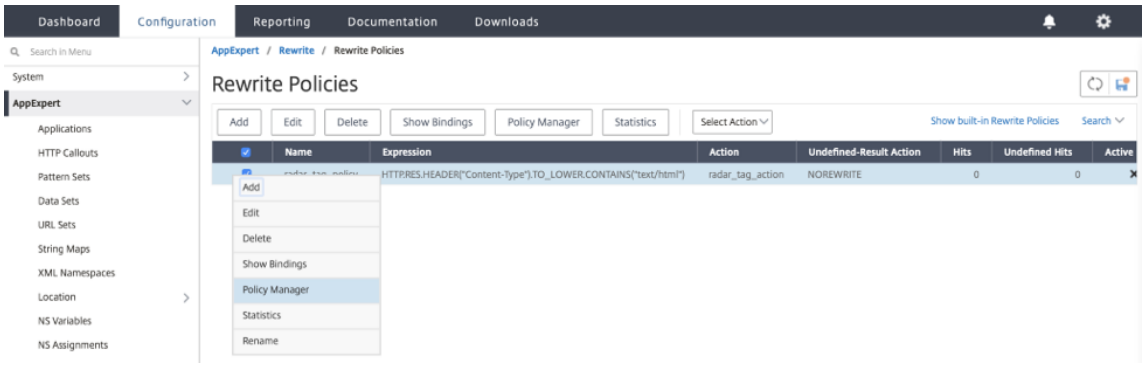


4. Haga clic en **Crear**.

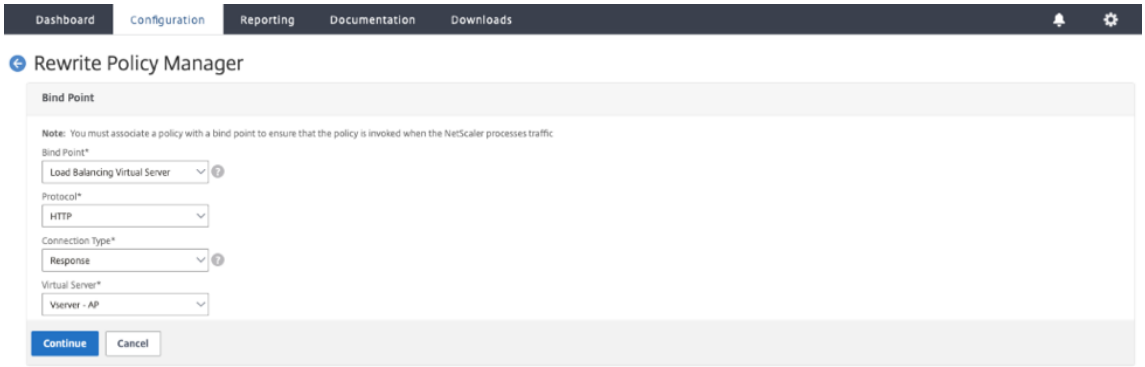
Ha completado la configuración de la directiva de reescritura.

Directiva de reescritura de enlace de GUI Una vez que haya terminado de configurar la directiva, el último paso es enlazar la directiva mediante el **Administrador de directivas**.

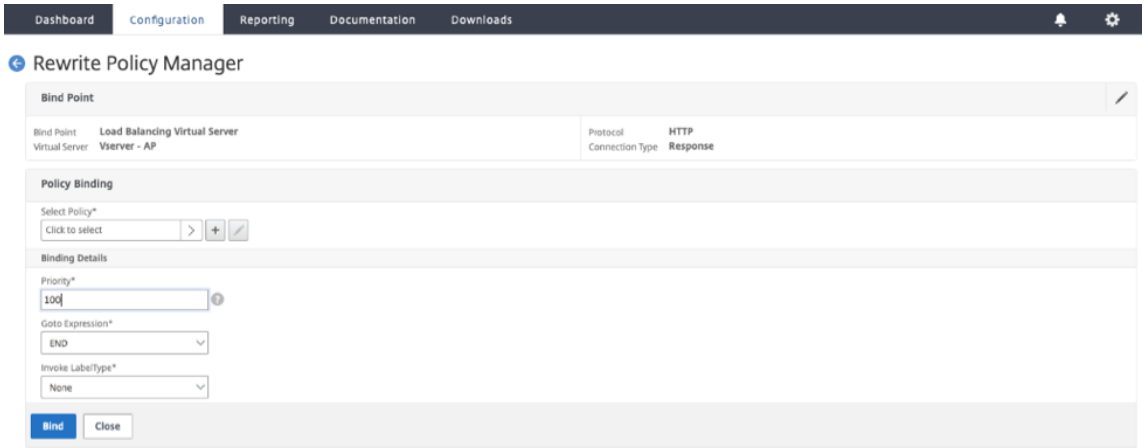
1. Vaya a la página **Volver a escribir directivas**.
2. Seleccione la directiva de reescritura que creó para la etiqueta de Radar.
3. Vaya al **Administrador de directivas**.



4. En la página **Administrador de directivas**, puede enlazar la directiva haciendo lo siguiente.
   - Para **Punto de enlace**, tiene la opción de seleccionar **Anular Global**, **Servidor Virtual VPN, Servidor VirtualContent Switching o ServidorVirtual de Equilibrio de carga**.
   - Para **Protocolo**, seleccione **HTTP**.
   - Para **Tipo de conexión**, seleccione **Respuesta**.
   - Para **Virtual Server**, use su propio nombre de servidor virtual.



- Haga clic en **Continuar**.
- En la página siguiente, seleccione la **directiva de reescritura** que creó anteriormente.
- Agregar **detalles de enlace**.
- Haga clic en **Bind**.

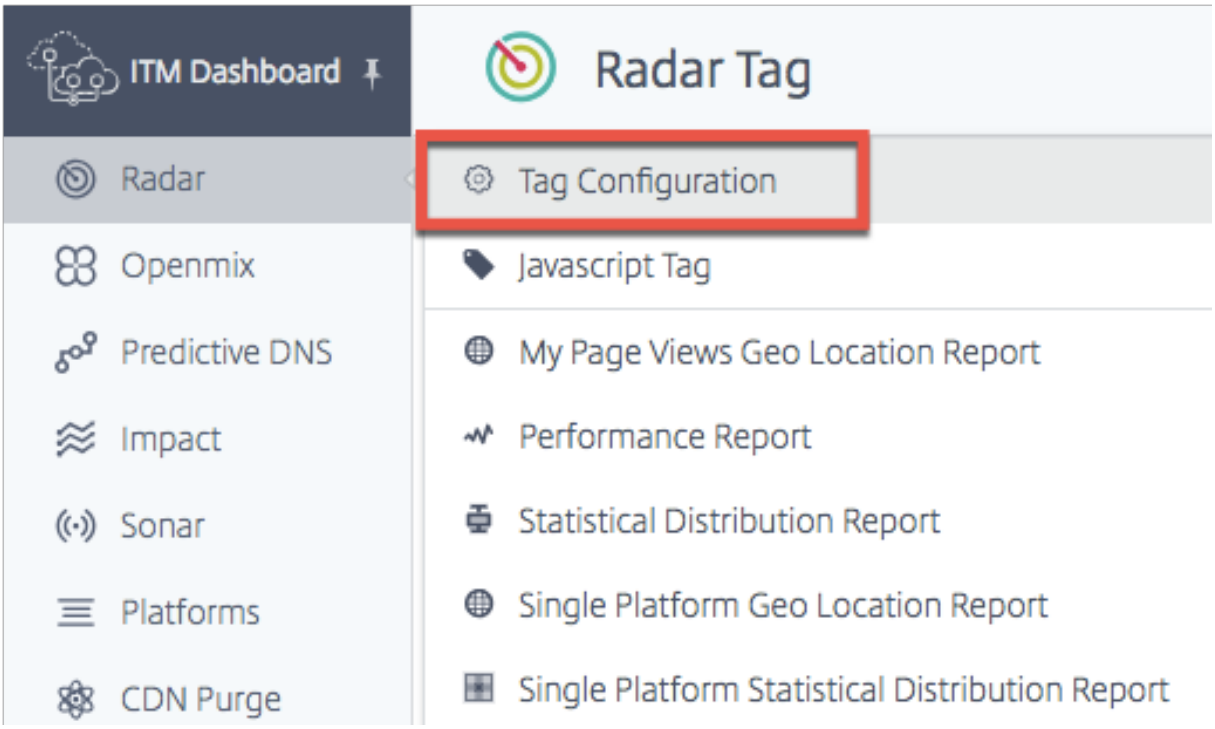


Con los métodos anteriores usted es capaz de insertar la etiqueta Radar en sus páginas web. Sin embargo, hay que señalar que se trata de una implementación básica. Se puede realizar un filtrado adicional para controlar mejor las páginas que tienen la etiqueta implementada.

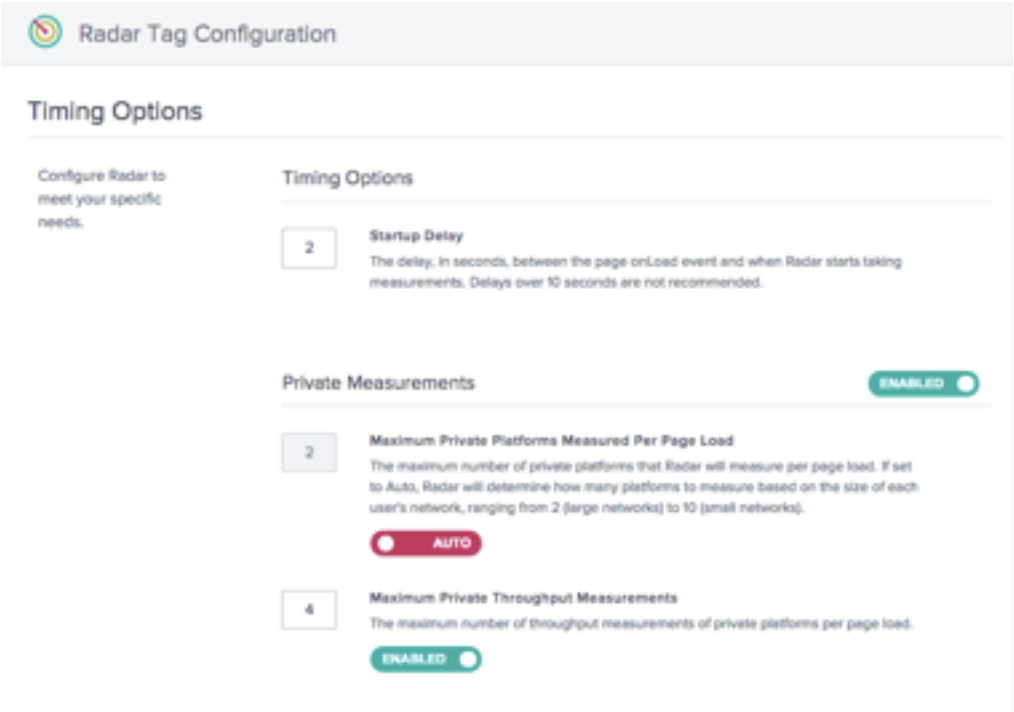
Configuración de la etiqueta de Radar

Puede configurar Radar en la página de **configuración de etiquetas de radar** .

1. Inicie sesión en el portal de administración inteligente del tráfico de NetScaler.
2. En el menú de navegación de la izquierda, seleccione **Radar > Configuración de etiquetas**.



Se abrirá la página Configuración de la etiqueta de Radar. Aquí puede configurar varias opciones para personalizar las mediciones de Radar. El JavaScript de Radar tiene parámetros que se pueden personalizar para ajustar los elementos de tiempo y retardo; número de pruebas completadas por los usuarios finales para mediciones comunitarias y privadas; y valores de tiempo de espera para medir la disponibilidad, etc.



En la siguiente tabla se proporciona información sobre las opciones de configuración y los valores predeterminados de cada una. Al realizar cambios, asegúrese de hacer clic en **Actualizar configuración de Radar** en la parte inferior de la pantalla para aplicar los cambios.

Función	Parámetro	Descripción	Configuración predeterminada
Opciones de temporización	Retraso de inicio	El retraso, en segundos, entre el evento onLoad de la página y cuando Radar registra el tiempo de navegación.	2 segundos
	Retraso de repetición	El retraso, en minutos, entre las sesiones de medición. Si el valor es mayor o igual a 5, la etiqueta Radar tomará más medidas después de cada intervalo de retardo de repetición. Si el valor es 0, la etiqueta de radar no tomará ninguna medida adicional.	5 minutos
Opciones de protocolo	Permitir siempre mediciones HTTPS privadas	Permite al cliente Radar tomar medidas HTTPS incluso desde un sitio web HTTP.	Realiza mediciones de plataformas con protocolos de URL que coinciden con la página en la que se ejecuta el cliente Radar.
	Permita mediciones HTTP privadas en conexiones HTTPS.	Permite al cliente Radar tomar medidas HTTP desde un sitio web HTTPS.	Realiza mediciones de plataformas con protocolos de URL que coinciden con la página en la que se ejecuta el cliente Radar.

Función	Parámetro	Descripción	Configuración predeterminada
Frecuencia de muestreo	Frecuencia de muestreo de Radar	El porcentaje de páginas en las que la etiqueta Radar está activada para realizar mediciones.	Inhabilitado
Medidas privadas	Medidas privadas máximas por carga de página	El número máximo de plataformas privadas que Radar medirá por carga de página.**	Automático*
	Mediciones de rendimiento privado máximo	El número máximo de mediciones de rendimiento de las plataformas privadas por carga de página.**	4
Medidas comunitarias	Medidas máximas de la comunidad por carga de página	El número máximo de plataformas comunitarias que Radar medirá por carga de página.**	Automático*
	Mediciones de rendimiento máximo de la comunidad	El número máximo de mediciones de rendimiento de las plataformas comunitarias por carga de página.**	4

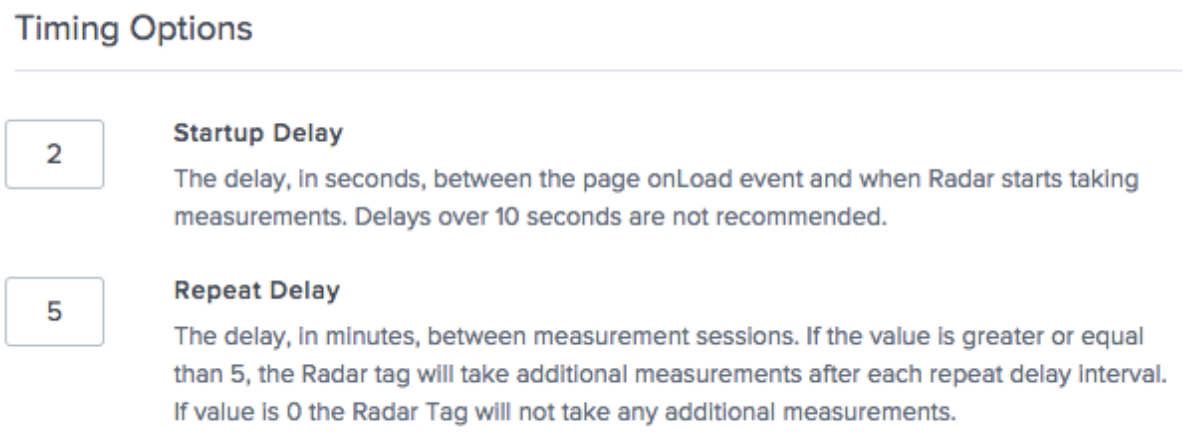
*Automático significa que NetScaler Intelligent Traffic Management determina cuántas plataformas deben medirse para una sesión determinada, en función de la ubicación del usuario final. Tratamos de medir más plataformas por sesión para redes pequeñas, donde los datos son escasos, en lugar de las redes grandes, donde son densos.

**Este es el número máximo de mediciones intentadas por sesión. Por ejemplo, Radar puede medir 4 plataformas privadas por sesión, todas ellas configuradas para medir tanto RTT como el rendimiento. Pero si las mediciones de rendimiento privado máximo se establecen en 2, el cliente dejará de incluir las mediciones de rendimiento después de medir las primeras 2 plataformas privadas. Para las dos últimas plataformas, solo medirá RTT.

Las opciones de temporización le permiten establecer la duración de tiempo que Radar debe esperar

antes de comenzar a tomar medidas.

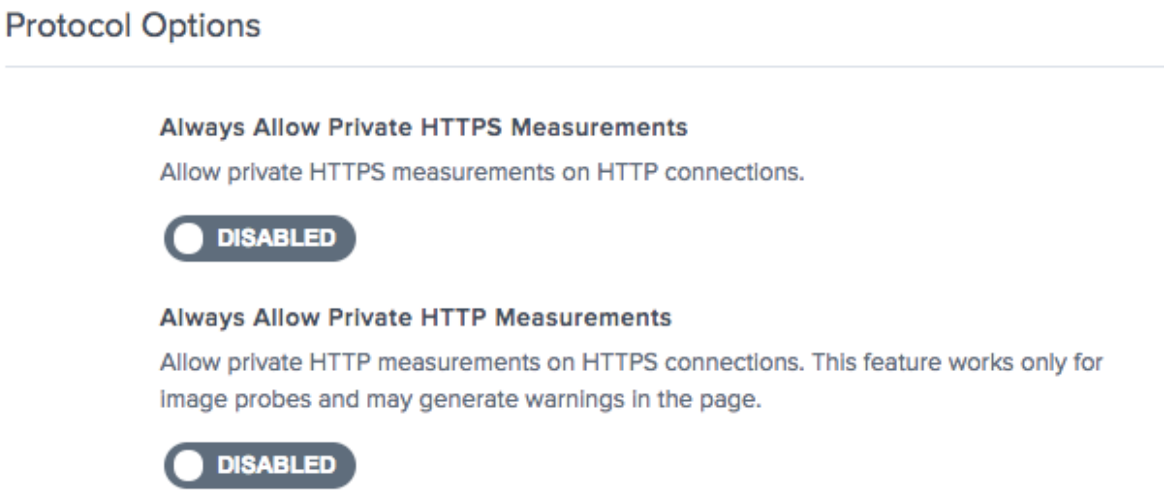
Nota: El retraso de inicio es en segundos, mientras que el **retraso de repetición** es en minutos.



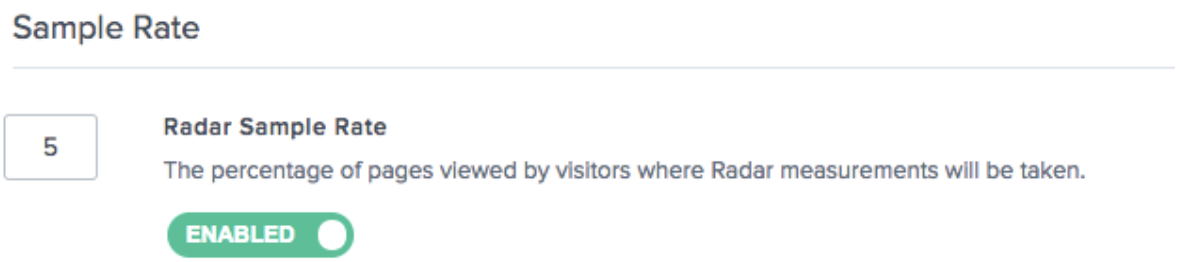
Opciones de protocolo

Normalmente, el cliente Radar solo mide plataformas con direcciones URL cuyos protocolos coinciden con los de la página donde se ejecuta. Estas opciones le permiten anular ese comportamiento para plataformas privadas. Por ejemplo, habilitar «Permitir siempre mediciones HTTPS privadas» permite al cliente medir `https://myprovider.com/r20.png` desde `http://example.com`, mientras que «Permitir siempre mediciones HTTP privadas» permite al cliente medir `http://myprovider.com/r20.png` desde `https://example.com`.

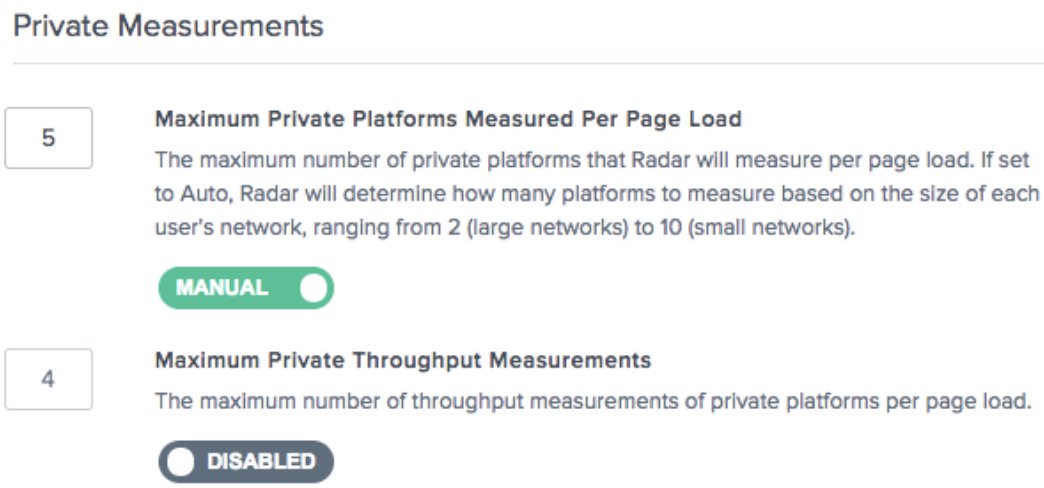
Por lo general, estas opciones deben evitarse excepto en casos de uso extremo. La mejor manera de asegurarse de obtener una densidad de medición privada adecuada es tener sus plataformas configuradas para medir las plataformas y protocolos que realmente utiliza en producción (y no más), y tener la etiqueta Radar implementada en tantas páginas de producción como sea posible. A veces nos referimos a esto como «Poner el radar donde se necesita». «



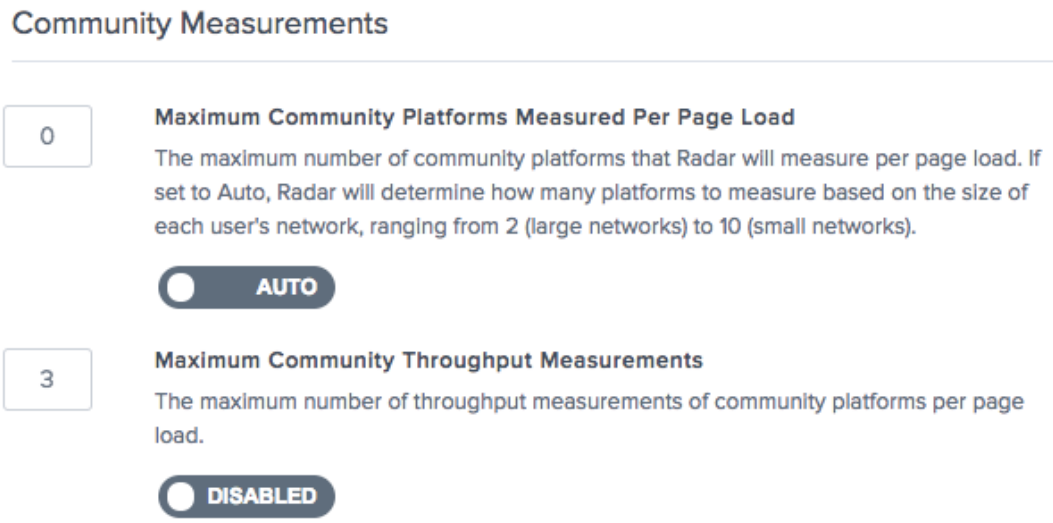
La frecuencia de muestreo le permite establecer un porcentaje de páginas web (vistas por los usuarios) para recopilar las mediciones. Por ejemplo, si su sitio web obtiene 100 000 páginas vistas al día y establece una tasa de muestreo del 5%, Radar solo recopilará mediciones del 5% de las 100 000 vistas de página.



Medidas privadas Esta configuración se aplica a las mediciones de sus plataformas privadas. Las plataformas privadas son aquellas que configura en la sección **Plataformas** para medir CDN específicos, proveedores de nube y otras partes de su infraestructura. Consulte la sección Plataformas para obtener más información.



Esta opción le permite configurar el comportamiento de Radar al proporcionar información a la comunidad.



Desactivar las pruebas de Radar

Si hay un requisito para desactivar rápidamente las mediciones de Radar en caso de que ocurra algo inesperado, puede hacerlo dentro del Portal para evitar cambios de código de emergencia en su sitio.

En la página Configuración de etiquetas de Radar, desactive Mediciones privadas, Mediciones de comunidad o ambas haciendo clic en el botón Activado para **Desactivado**.

Haga clic en **Guardar configuración de Radar** para confirmar los cambios. Los cambios pueden tardar uno o dos minutos en propagarse después de lo cual las mediciones del Radar se detienen.

Mediciones comunitarias

Metodología del cliente de Radar

Una dimensión fundamental del comportamiento del cliente es la **sesión**. Todos los datos que envía el cliente están asociados a una sesión. Las sesiones se crean realizando una llamada a los servidores ITM de NetScaler, conocida como solicitud de inicialización. Las sesiones caducan con bastante rapidez, lo que ayuda a garantizar que solo se acepten datos Radar válidos. Gracias a esta función, las mediciones de radar siempre vienen en lotes asociados a su ID de transacción de sesión y, a menudo, nos referimos a una «sesión de radar» para describir las mediciones asociadas a ella.

Sesión de Radar

Una sesión de Radar es la unidad principal de trabajo que realiza el cliente. Consiste en una solicitud a los servidores ITM de NetScaler para obtener la configuración del cliente y un conjunto de plataformas para medir, seguida de solicitudes para medir esas plataformas e informar de los resultados. Estos tienen lugar de forma asíncrona y serializada, de modo que solo se realiza una solicitud a la vez.Una sesión típica se completa en menos de 10 segundos.

Tipos de sondeo

Cada informe que envía el cliente tiene un tipo de sonda asociado, que indica al sistema qué tipo de medida es y cómo tratarla. También indica los tipos de mediciones que se realizarán, que pueden incluir disponibilidad, tiempo de ida y vuelta, rendimiento u otra recopilación de métricas.

Existe una relación importante entre la disponibilidad y el sondeo del rendimiento (como el tiempo de ida y vuelta y el rendimiento). La disponibilidad de un recurso en particular siempre se mide primero en una sesión de medición concreta. Solo si la medición de disponibilidad se realiza correctamente, se pueden realizar mediciones de rendimiento adicionales del mismo recurso en esa misma sesión. «

Si una red particularmente lenta sufre una interrupción de disponibilidad, esto puede dar como resultado el rendimiento agregado de los informes que incluyen esta red para mejorar realmente. Esto es solo un artefacto de generación de informes, ya que NetScaler Intelligent Traffic Management siempre utiliza los datos de rendimiento más detallados y específicos de la red para tomar decisiones en tiempo real.

Disponibilidad La disponibilidad también conocida como sondeos de arranque en frío está pensada para permitir que los servicios calienten sus cachés. Aunque hay un valor de medición asociado con este sondeo. Utilizamos el sondeo de disponibilidad para determinar si el proveedor está disponible.

Si una plataforma no está configurada para realizar un sondeo de arranque en frío, utilizamos los resultados del sondeo RTT en lugar de un informe de arranque en frío para proporcionar métricas de disponibilidad.

Del mismo modo, para los objetos dinámicos que miden los servicios de aceleración del sitio, el cliente descarga el objeto de prueba pequeño una vez e informa del valor de medición tanto para el inicio en frío como para el tiempo de respuesta.

Objeto de prueba	Definición
Estándar	Uso de marcas de tiempo de tiempo de recursos: responseStart - requestStart
Dinámico	Uso de marcas de tiempo de tiempo de recursos: responseEnd - domainLookUpStart

RTT

Objeto de prueba	Intervalo	API	Descripción
Estándar	ResponseStart - RequestStart	Temporización de recursos	Tiempo para que se devuelva un solo paquete en respuesta a una solicitud HTTP.
Dinámico	responseEnd - DomainLookUpStart	Temporización de recursos	El tiempo de una solicitud que se va a servir, incluido el tiempo de búsqueda DNS, el tiempo de conexión y el tiempo de respuesta.

Rendimiento

Objeto de prueba	Intervalo	API	Descripción
Estándar	Tamaño del archivo (kilobytes) * 8/(responseEnd - requestStart)	Temporización de recursos	El rendimiento medido (kilobits por segundo) para una solicitud y respuesta completa basada en una descarga de objetos de prueba grande.
Dinámico	Tamaño del archivo (kilobytes) * 8/(responseEnd - domainLookUpStart)	Temporización de recursos	El rendimiento medido (kilobits por segundo) para una solicitud y respuesta completa basada en una descarga de objetos de prueba grande. Normalmente, esto no incluye el tiempo de conexión ni el tiempo de búsqueda DNS en caso de que ya se haya descargado un objeto de prueba RTT.

Objetos de prueba

Los objetos de prueba son archivos alojados en plataformas y descargados por el cliente para generar mediciones. En esta sección se describen los diferentes tipos de objetos de prueba que admite el cliente. No todos los tipos de objetos se aplican a todas las plataformas.

Encabezado requerido:

El encabezado de respuesta Timing-Allow-Origin es necesario para permitir el acceso de JavaScript a los datos de temporización de bajo nivel suministrados por la API Resource Timing. La configuración recomendada es la `Timing-Allow-Origin: *`siguiente: se debe conceder permiso para acceder a los datos de temporización del recurso a JavaScript que se ejecute en cualquier dominio.

Estándar Los objetos de prueba estándar son medios, que el cliente descarga estableciendo el`src` atributo en un objeto Image. Una vez descargado, el cliente utiliza la API de sincronización de recursos para recopilar datos de rendimiento.

Estos objetos de prueba deben ser servidos con el encabezado de respuesta Timing-Allow-Origin. Consulte la sección **Timing-Allow-Origin Encabezado** para obtener más información.

Estándar pequeño El pequeño objeto de prueba estándar es un archivo de imagen de un solo píxel, que se utiliza cuando el cliente necesita realizar una solicitud de red ligera.

El objeto de prueba pequeño estándar se utiliza en los siguientes casos de uso:

- Sondas de arranque en frío no dinámicas
- Sondas de tiempo de ida y vuelta no dinámicas

Estándar Grande El objeto de prueba grande estándar es un archivo de imagen de 100 KB utilizado para medir el rendimiento de una plataforma.

Nombres de objetos grandes: para calcular el rendimiento, el cliente necesita saber el tamaño del objeto de prueba.El cliente determina el nombre del archivo buscando KB en algún lugar del nombre del archivo;`r20-100KB.png`, por ejemplo. Los clientes pueden medir archivos de imagen de diferentes tamaños siempre y cuando el nombre contenga el tamaño de archivo de la misma manera, por ejemplo`myimage-2048kb.jpg`.

Dinámico Los objetos de prueba dinámicos se utilizan para medir el rendimiento asociado con los servicios de aceleración de sitio.
Cada uno es un archivo HTML que contiene JavaScript capaz de recopilar marcas de tiempo de la API de sincronización de navegación y publicarlas en la página principal. El cliente descarga el objeto de prueba utilizando un iframe y obtiene estas marcas de tiempo, que utiliza para calcular las mediciones.

Seguridad y validación El objeto de prueba es un objeto de 40 KB. Una nueva función del objeto de prueba es un HMAC (código de autenticación de mensajes basado en hash) que proporciona basado en parámetros de consulta y una clave secreta a la que el servidor tiene acceso. Este HMAC se envía de vuelta con nuestra medición, lo que nos permite validar que el cliente de Radar pudo acceder al objeto de prueba y no se almacenó nada en caché.

Diferencia entre objetos de prueba dinámicos y estándar:

Para las mediciones de Radar estándar, tratamos de aislar solo la actividad de solicitud principal asociada con la descarga de objetos de prueba, mientras que para los servicios de aceleración de sitio nuestro objetivo es medir más de la actividad. Por lo tanto, la búsqueda DNS y el tiempo de conexión también se incluyen.
Además, las mediciones dinámicas están destinadas a medir el rendimiento de la solicitud al acceder al origen del servicio, no solo a una caché de borde.

En el Portal, puede elegir esta metodología haciendo lo siguiente:

- En el menú de navegación de la izquierda, vaya a **Plataformas**.
- Haga clic en el icono **Agregar plataforma** en la esquina superior derecha de la página.
- Vaya a **Plataforma privada > Categoría > Contenido dinámico**.
- En el cuadro de diálogo **Objetos de prueba de Radar**, haga clic en la casilla de verificación **Personalizar sondas**.
- Introduzca la url **Tiempo de respuesta** y seleccione **Dinámica de página web** en la lista implementable **Tipo de objeto**.

El objeto de prueba pequeño dinámico se utiliza para medir la disponibilidad y el tiempo de ida y vuelta utilizando el mismo sondeo para los servicios de aceleración de sitio.

En AV El objeto de prueba iNav es un archivo HTML estático que contiene JavaScript capaz de realizar una serie de tareas. El cliente indica qué tarea le gustaría realizar incluyendo parámetros de cadena de consulta en la URL que carga el archivo HTML en un iframe.
El objeto de prueba iNav admite los siguientes casos de uso:
iNav arranque en frío
iNav tiempo de ida y vuelta

iUni El objeto de prueba iUNI se utiliza para detectar el valor UNI asociado con un conjunto de mediciones de Radar para una plataforma (el otro método es CORS AJAX que no requiere un objeto de prueba separado).

AJAX GET La metodología AJAX GET generalmente se puede usar con cualquier URL que el cliente desee medir, siempre que se sirva con el encabezado **Timing-Allow-Origin** y un encabezado **Access-Control-Allow-Origin** apropiado.
En el Portal, puede elegir esta metodología haciendo lo siguiente:

- En el menú de navegación de la izquierda, vaya a **Plataformas**.
- Haga clic en el icono **Agregar plataforma** en la esquina superior derecha de la página.
- Vaya a **Plataforma privada > Categoría > Contenido dinámico**.
- En el cuadro de diálogo**Objetos de prueba de Radar**, haga clic en la casilla de verificación **Personalizar sondas**.
- Introduzca el **tiempo de respuesta** y elija **AJAX (GET)** en la lista implementable **Tipo de objeto**.

Encabezado de Timing-Allow-Origin El encabezado de respuesta Timing-Allow-Origin es necesario para permitir el acceso de JavaScript a los datos de temporización de bajo nivel suministrados por la API Resource Timing.

La configuración recomendada es `Timing-Allow-Origin: *`, que indica que se debe conceder permiso para acceder a los datos de temporización del recurso a JavaScript que se ejecute en cualquier dominio.

API de Radar

Radar proporciona API para funciones operativas y de recuperación de datos.

- API de operaciones: Agregar/Modificar/Eliminar cuentas de Radar y los mecanismos de control para ejecutar su cuenta a través de una API
- API de datos de Radar: La API de datos de Radar de ITM proporciona agregados de la comunidad pública de Radar y datos de medición privados. Los datos se actualizan continuamente y se almacenan por lotes aproximadamente cada 60 segundos para que la API los recupere. La API de datos se proporciona para permitir a los clientes integrar datos de Radar en sus propios informes y paneles. Una sola llamada a la API puede proporcionar cuartil Radar o medias de mediciones de medianas para todos los países y hasta 30 ASN de interés, para cada plataforma.

Informes de Radar

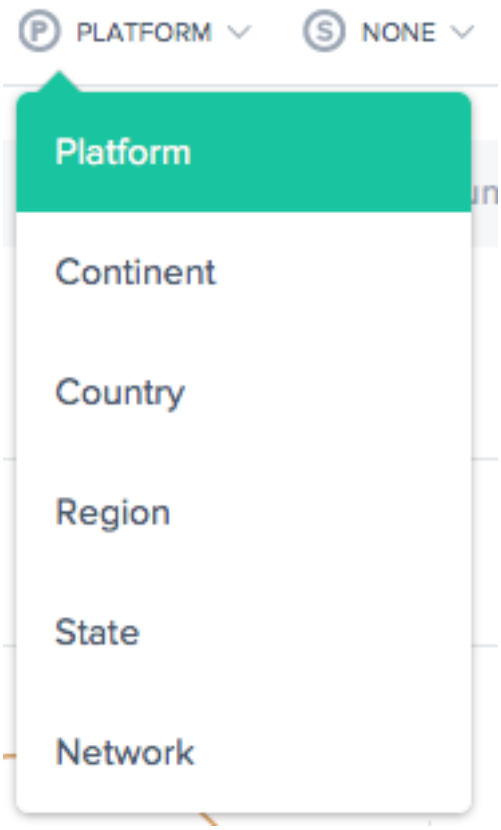
Los informes de Radar proporcionan una potente visibilidad de los datos dinámicos recopilados a través de la etiqueta de Radar.

Los miembros del Radar tienen acceso a un rico conjunto de datos presentado a través de gráficos interactivos intuitivos. El conjunto de datos recopilado incorpora tanto el conjunto completo de datos públicos de miles de millones de mediciones como un contexto para los datos privados recopilados desde la etiqueta Radar de un cliente o la implementación de SDK móvil. La información del tiempo de carga de página se captura con la etiqueta del cliente, lo que proporciona una visión profunda de la experiencia real de rendimiento de su sitio web y de los usuarios finales de aplicaciones móviles.

Además de las métricas de rendimiento, los informes de Radar proporcionan información sobre muchas facetas de su audiencia de usuario final, incluyendo: volúmenes, geografías, agentes de usuario, tipos de SO y el momento en que utilizan su sitio web o aplicación móvil.

Cada informe se define a continuación, pero aquí hay aspectos importantes de todos los informes:

Cotas primaria y secundaria



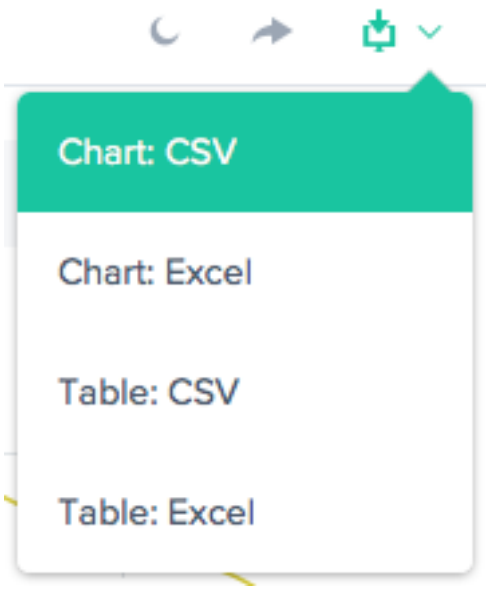
La dimensión principal del gráfico se selecciona mediante una lista de selección de lista situada encima del gráfico. Utilice esto como un potente pivote en el informe. También se puede elegir una dimensión secundaria para refinar aún más los informes.

Alternar fondo de visualización

Alternar

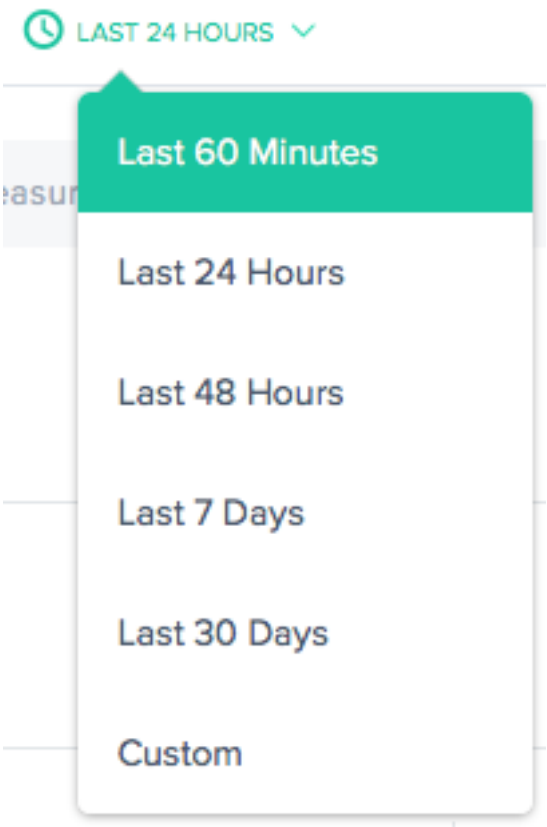
Los gráficos se establecen en un fondo blanco de forma predeterminada. Alternar el fondo a un color oscuro para los monitores de alto contraste mediante la alternancia de fondo.

Exportación de datos



Además, el usuario final puede descargar los datos del gráfico y de la tabla a través del enlace de descarga en la parte superior del informe.

Filtro: Rango de tiempo del informe



Los informes de Radar se pueden generar con un rango de tiempo de últimos 60 minutos, últimas 24 horas, últimas 48 horas, últimos 7 días, últimos 30 días o un rango personalizado. La vista predeterminada es las últimas 24 horas.

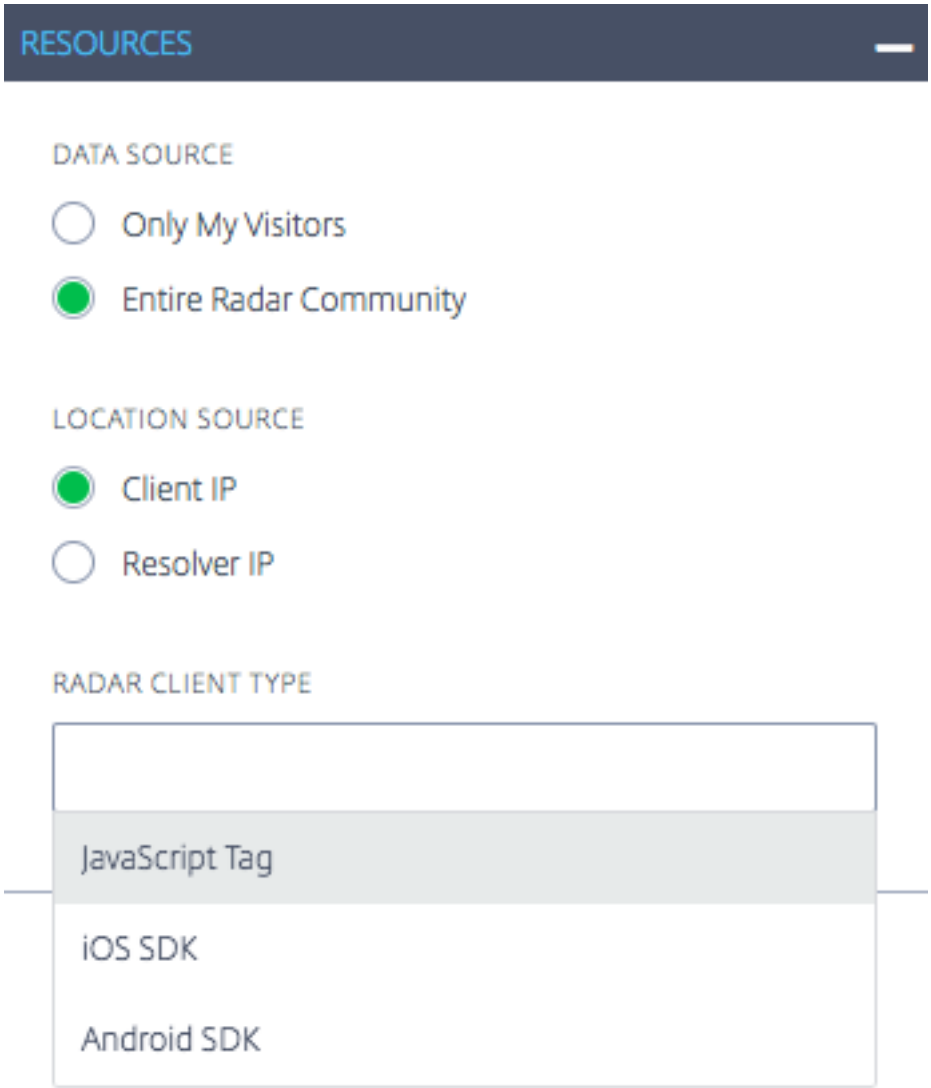
Filtro: Plataforma y Ubicación

Los informes varían ligeramente en términos de qué filtros son apropiados en función de los datos. Los siguientes son los más comunes:

- **Plataforma**: Seleccione una o más plataformas (proveedor) para incluir.
- **Continente**: Seleccione uno o más continentes para incluir.
- **País**: Seleccione uno o más países para incluir.
- **Región**: Seleccione una o más regiones geográficas (cuando corresponda) que quiera incluir.
- **Estado**: Seleccione uno o más estados geográficos (cuando corresponda) para incluirlos.
- **Red**: Seleccione una o más redes (ASN) que quiere incluir.

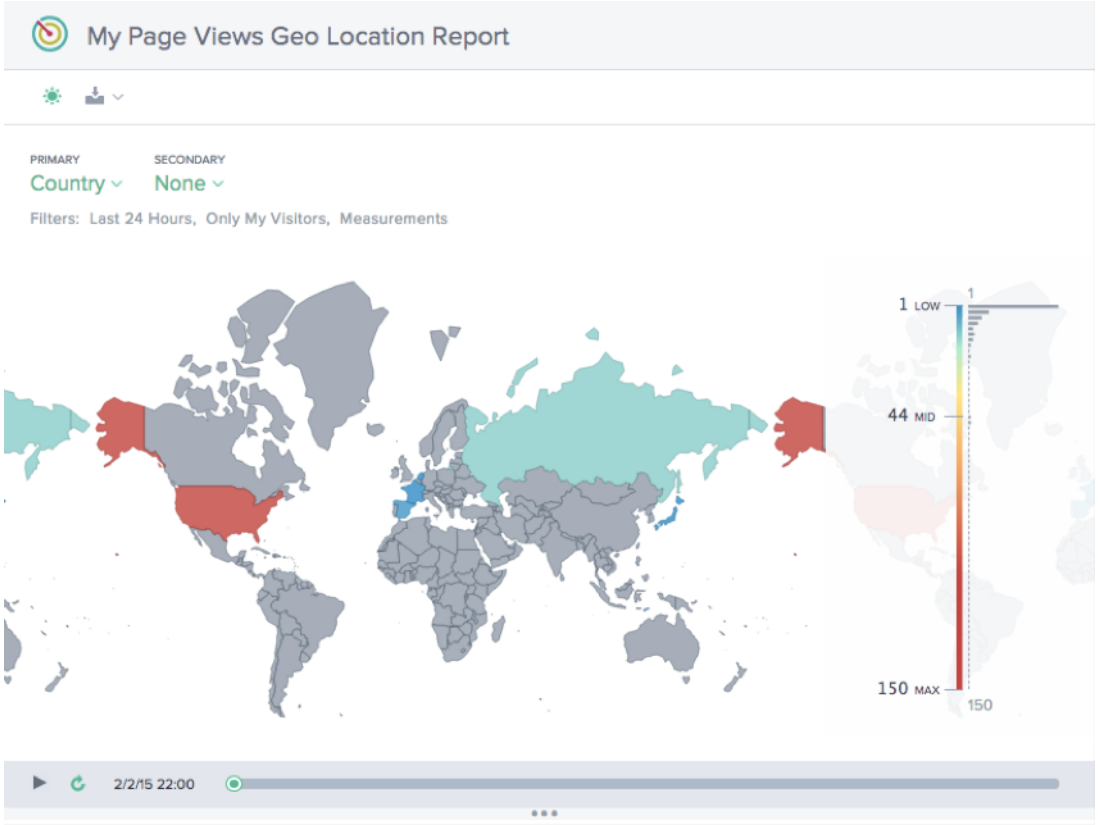
Filtrar: Recursos

- **Fuente de datos** : incluya datos de toda la comunidad de Radar o solo de los visitantes de su sitio.
- **Origen de ubicación**: Seleccione la IP del cliente o la IP de resolución como su origen de ubicación.
- **Tipo de cliente de** Radar: seleccione el tipo de cliente de Radar como una etiqueta JavaScript, SDK de iOS o SDK de Android.



Informe de ubicación geográfica de mis vistas de página

Este informe muestra el volumen de páginas vistas de cada país. Esta vista de mapa se puede ver a lo largo del tiempo (según el intervalo de tiempo elegido para el informe) seleccionando el botón **"Reproducir"** en la parte inferior del gráfico.

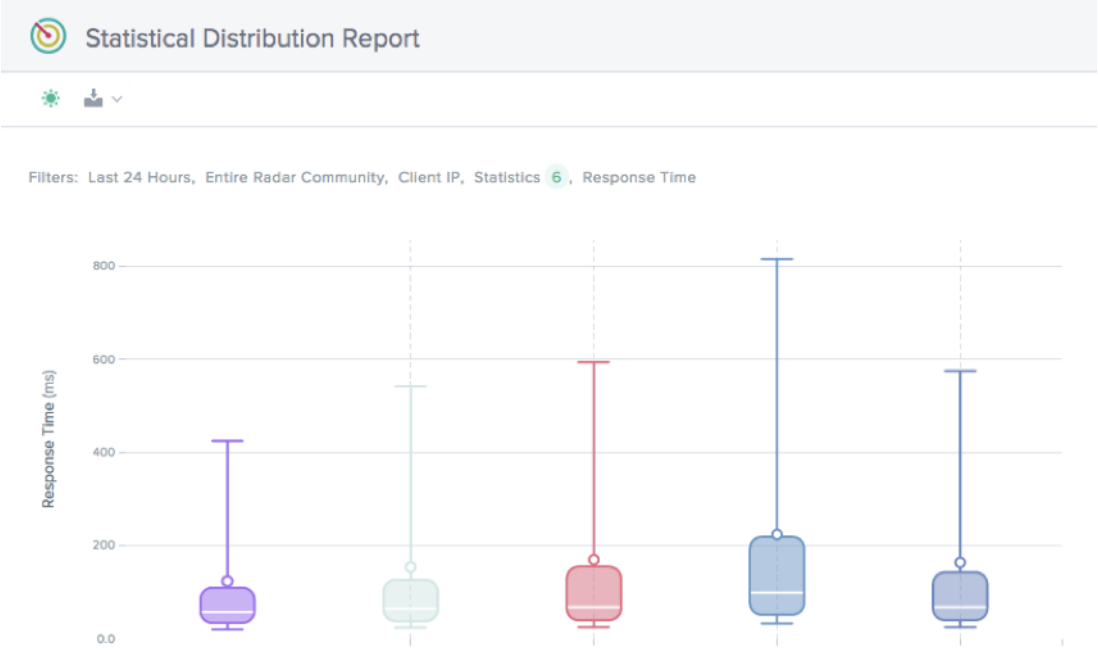


Informe de rendimiento

Este informe muestra la tendencia de rendimiento para cada una de las Plataformas definidas.

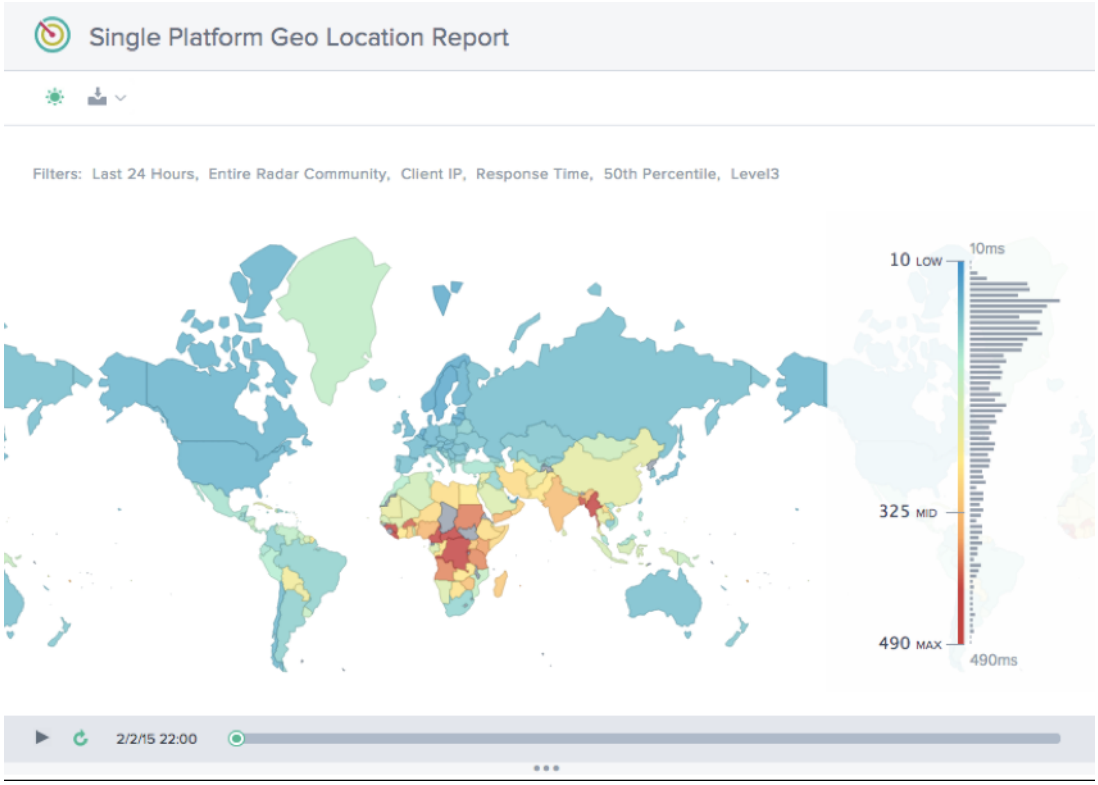
Informe de distribución estadística

Este informe muestra el desglose estadístico de cada una de las Plataformas definidas para la cuenta.



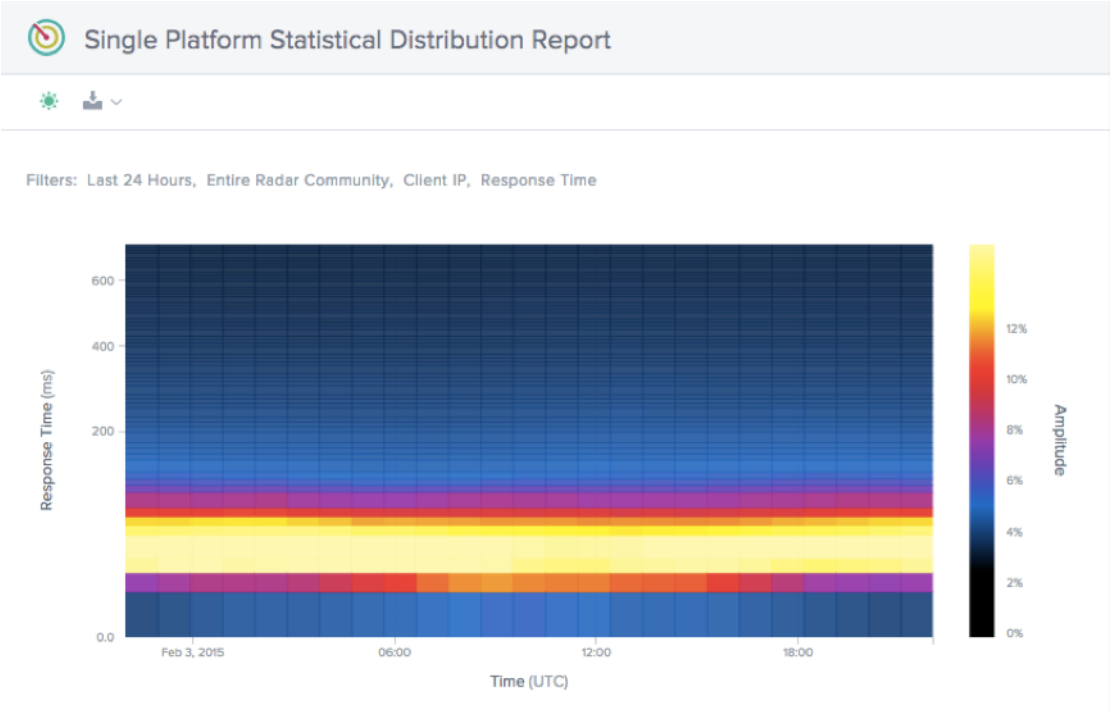
Informe de ubicación geográfica de una plataforma única

Este informe muestra la distribución del tráfico de Radar por país a lo largo del tiempo para una sola plataforma a la vez.



Informe de distribución estadística de plataforma única

Este informe muestra la distribución del tráfico de Radar a lo largo del tiempo por tiempo de respuesta.

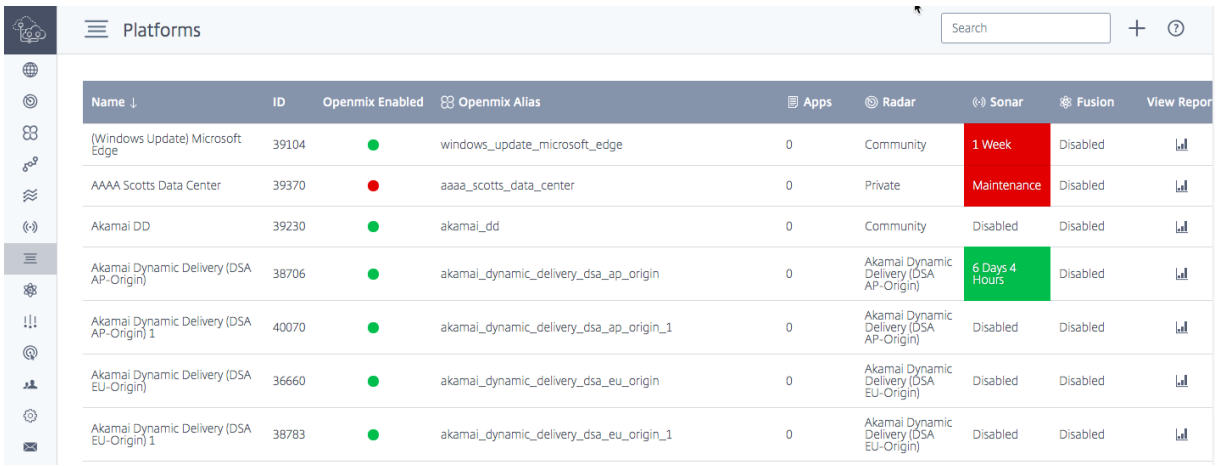


Plataformas

January 10, 2022

La página **Plataformas** es donde el cliente especifica los CDN, las nubes, los centros de datos u otros puntos finales que deben ser supervisados y utilizados con Openmix. Se debe configurar una plataforma para cada punto final de enrutamiento en el que desee informar. La mayoría de las veces, una plataforma representa una CDN, una región en la nube o una instancia individual, si usa Openmix para GSLB.

Al hacer clic en este elemento de menú, se presenta al cliente la siguiente pantalla.



Esta pantalla muestra una lista completa de todas las plataformas configuradas para informes, mediciones de Radar o los servicios de Sonar y Fusion.

La tabla muestra:

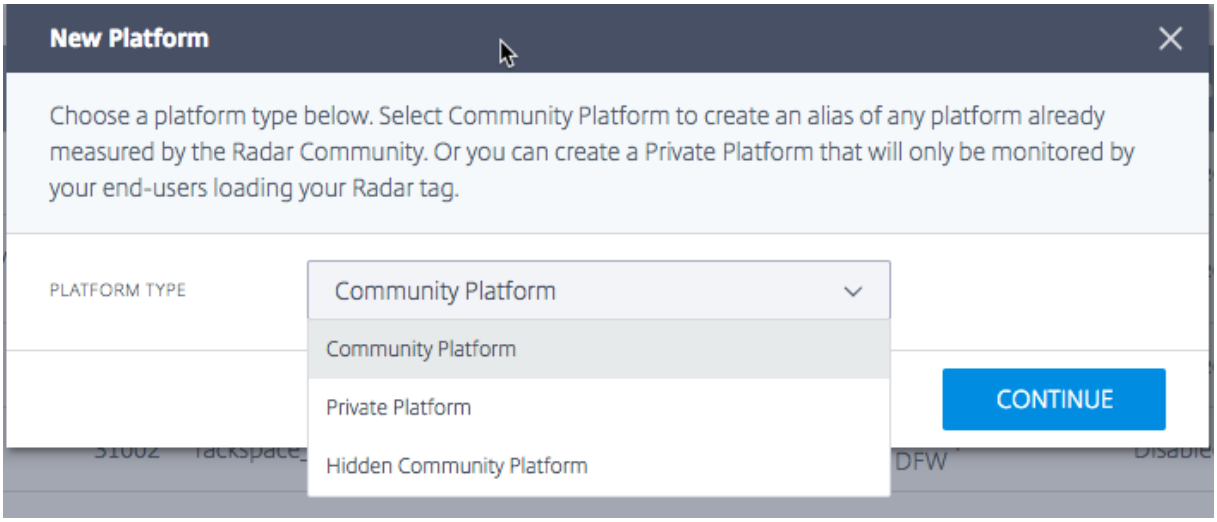
Se dirige	Descripción
Nombre	Nombre definido por el usuario de la plataforma.
IDENTIFICACIÓN	El ID generado para la plataforma, útil para el acceso a API y la generación de informes.
Alias de Openmix	El alias con el que hacer referencia a la plataforma desde las aplicaciones Openmix.
Aplicaciones	El número de aplicaciones Openmix que utilizan la plataforma.
Radar	Si la plataforma está configurada para usar mediciones de Radar comunitarias o privadas.
Sonar	Si Sonar está activado en esta plataforma.
Fusion	Si Fusion está activado en esta plataforma.

Creación de una plataforma

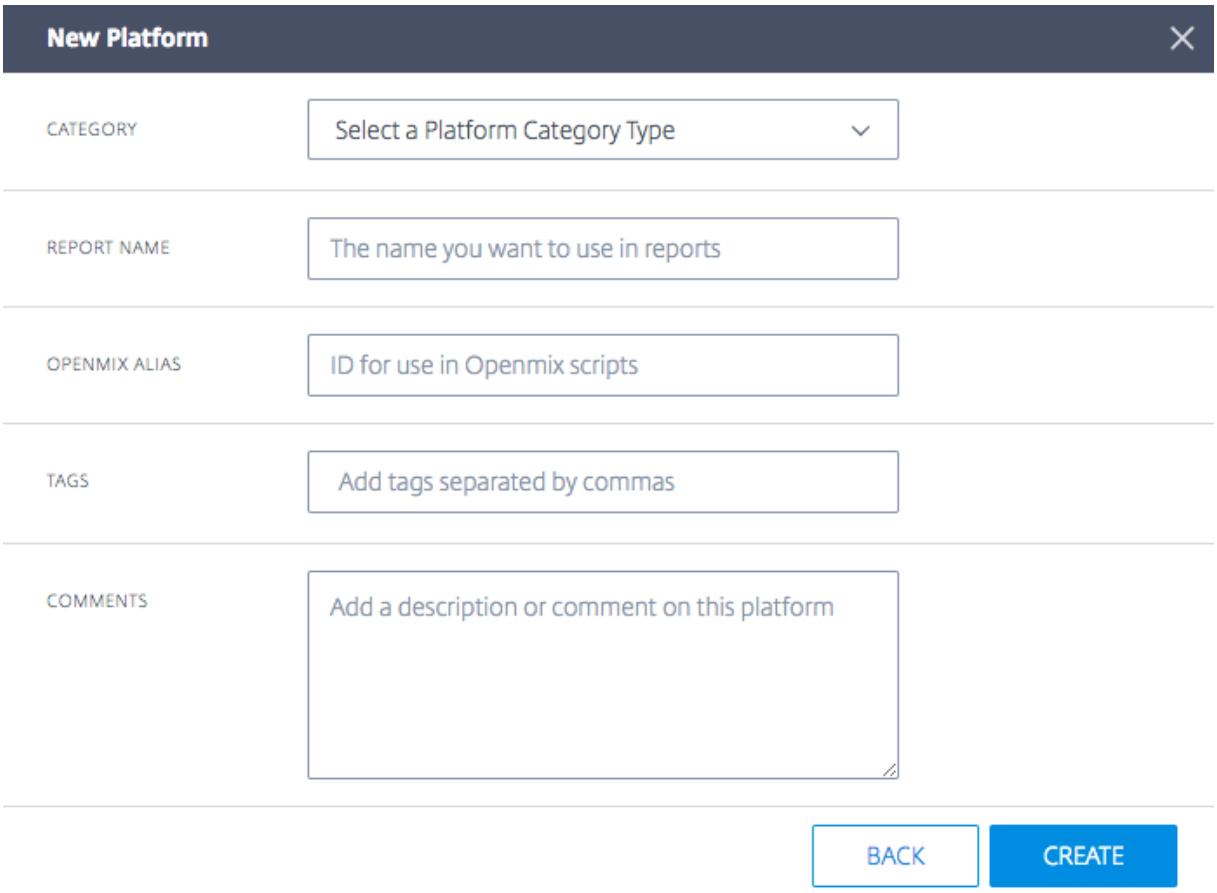
Para agregar una plataforma, haga clic en el botón **+** situado en la parte superior de la página Plataformas.

Nuevas Plataformas

Una vez que haya hecho clic en **Agregar plataformas**, verá la siguiente página donde puede seleccionar el tipo de plataforma que desea configurar.



Una vez que seleccione el **tipo de plataforma**, puede proporcionar un nombre para la plataforma que se utilizará para mostrar información y se utilizará en otros servicios que ITM proporciona, como Openmix.

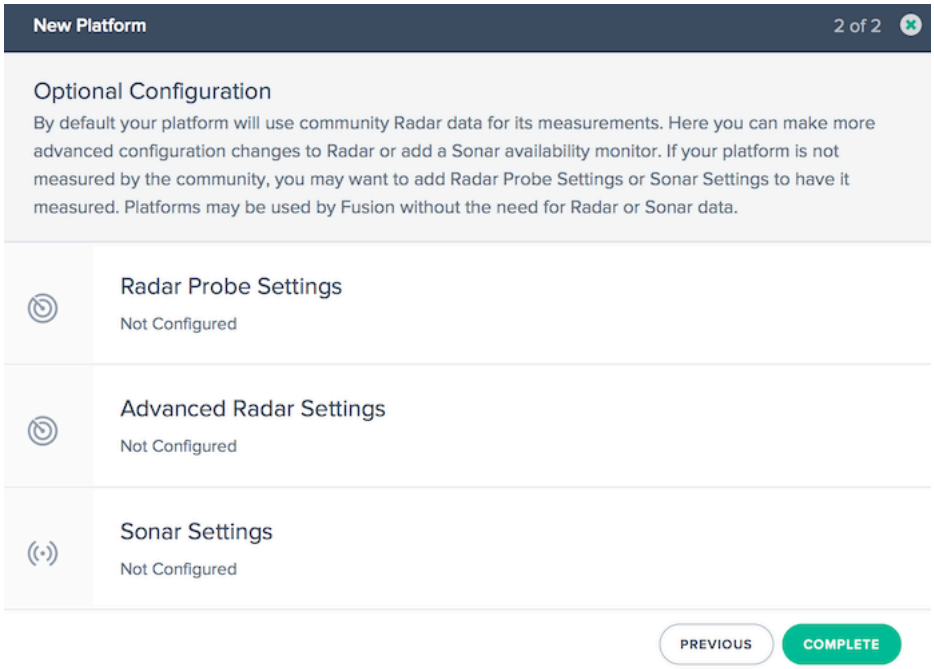


En **Configuración de la plataforma**, introduzca la siguiente información:

Elemento de entrada	Descripción
Categoría	El tipo de servicio que representa la plataforma. Las plataformas se manejan de manera diferente en Radar y Openmix, dependiendo del tipo. Las categorías de plataforma disponibles son: Cloud Computing, Dynamic Content, Delivery Networks, Cloud Storage, Secure Object Delivery y Managed DNS. Para las plataformas **privadas**, una categoría más disponible es **Data Center**. Nota: Todas las GSLB importadas se crean como centros de datos.
Plataforma	Seleccione la plataforma que desea probar, por ejemplo, Akamai, Amazon, Azure, etc.
Nombre del informe	Nombre de la plataforma utilizada en la presentación y presentación de informes.
Alias de Openmix	El alias que usan las aplicaciones Openmix para identificar la plataforma.
Etiquetas	Las etiquetas se pueden asignar a las plataformas para que puedan organizarse según sea necesario.

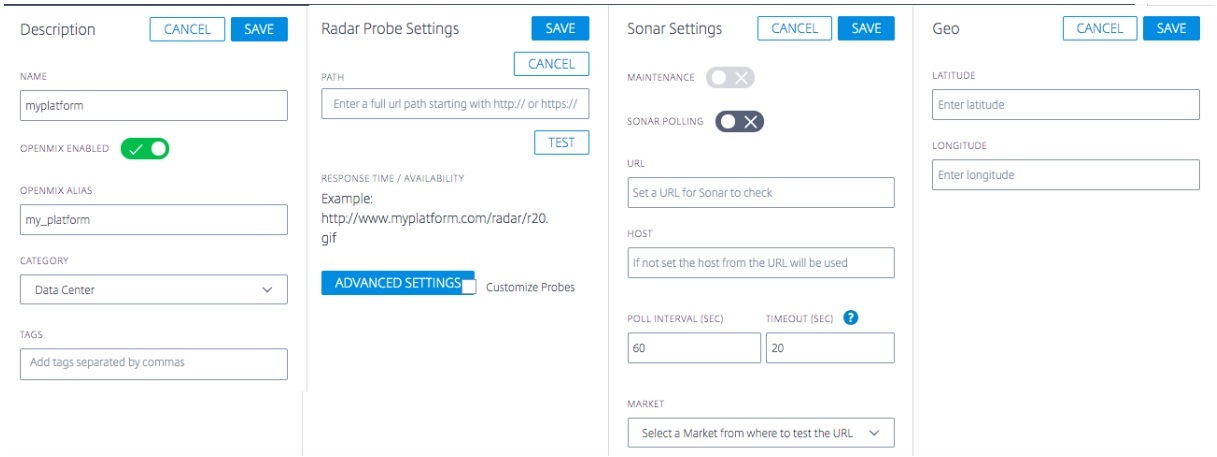
Cuando selecciona una plataforma existente, se rellenan los campos **Nombre del informe y Alias de Openmix**. Puede dejar estos campos con los valores predeterminados o modificarlos como prefiera.

Haga clic en **Siguiente** para continuar con la configuración opcional. Cuando haya terminado con la configuración opcional, haga clic en **Completar** para agregar la plataforma.



Edición de una plataforma

Modificar una plataforma es tan fácil como hacer clic en la fila de la plataforma en la tabla y hacer clic en el botón **Modificar**.



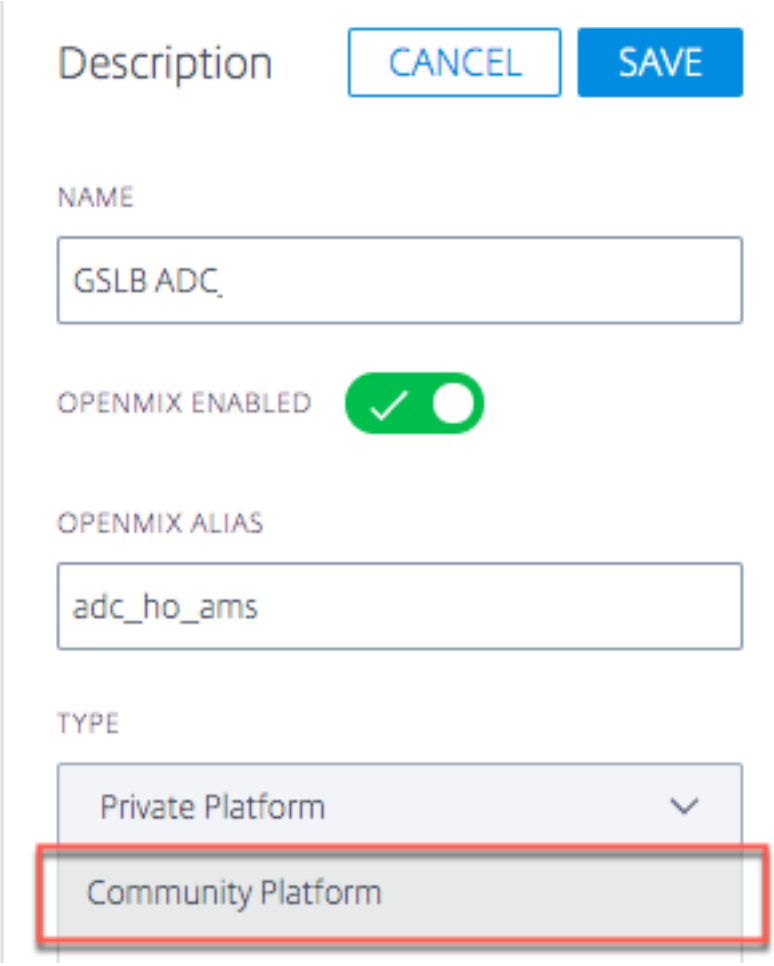
Una vez que haya cambiado la configuración, simplemente haga clic en **Guardar**, como lo haría con una nueva aplicación y esto le llevará de vuelta a la pantalla de plataformas con los cambios guardados.

Cambiar tipo de plataforma

Esta función es útil para los clientes cuyas plataformas privadas están alojadas en un centro de datos público o en una región de nube medida por la comunidad de Radar (AWS, por ejemplo) y desean heredar los datos de Radar de esa plataforma de la comunidad. Por ejemplo, cuando los clientes importan GSLB en el portal ITM, se importan como centros de datos privados, pero en realidad pueden ubicarse en una región de nube pública. Para heredar los datos de Radar de la plataforma de la comunidad, los clientes pueden cambiar la configuración actual de la plataforma privada o GSLB para hacer referencia a la plataforma de la comunidad en su lugar.

Para cambiar el tipo de plataforma, como un GSLB o un centro de datos privado, a una plataforma de comunidad pública (o de comunidad a privada si es necesario), haga lo siguiente.

1. Haga clic en la fila de la plataforma de la tabla **Plataformas**.
2. En la sección **Configuración de la plataforma**, haga clic en el botón **Modificar**.
3. Vaya a **Tipo**. Seleccione **Plataforma comunitaria** de la lista si desea cambiar su plataforma privada a una plataforma comunitaria.
4. Vaya a **Categoría**. Elija una categoría de plataforma de la lista.
5. Vaya a **Plataforma**. Seleccione la plataforma a la que desea cambiar en la lista implementable **Plataforma**.
6. Haga clic en **Guardar** en la parte superior derecha de la sección **Configuración de la plataforma**. Verá un mensaje de confirmación que le indica que la configuración de la sonda de Radar para su plataforma privada se eliminará y reemplazará por la configuración de la plataforma de la comunidad.
7. Haga clic en **Confirmar**.

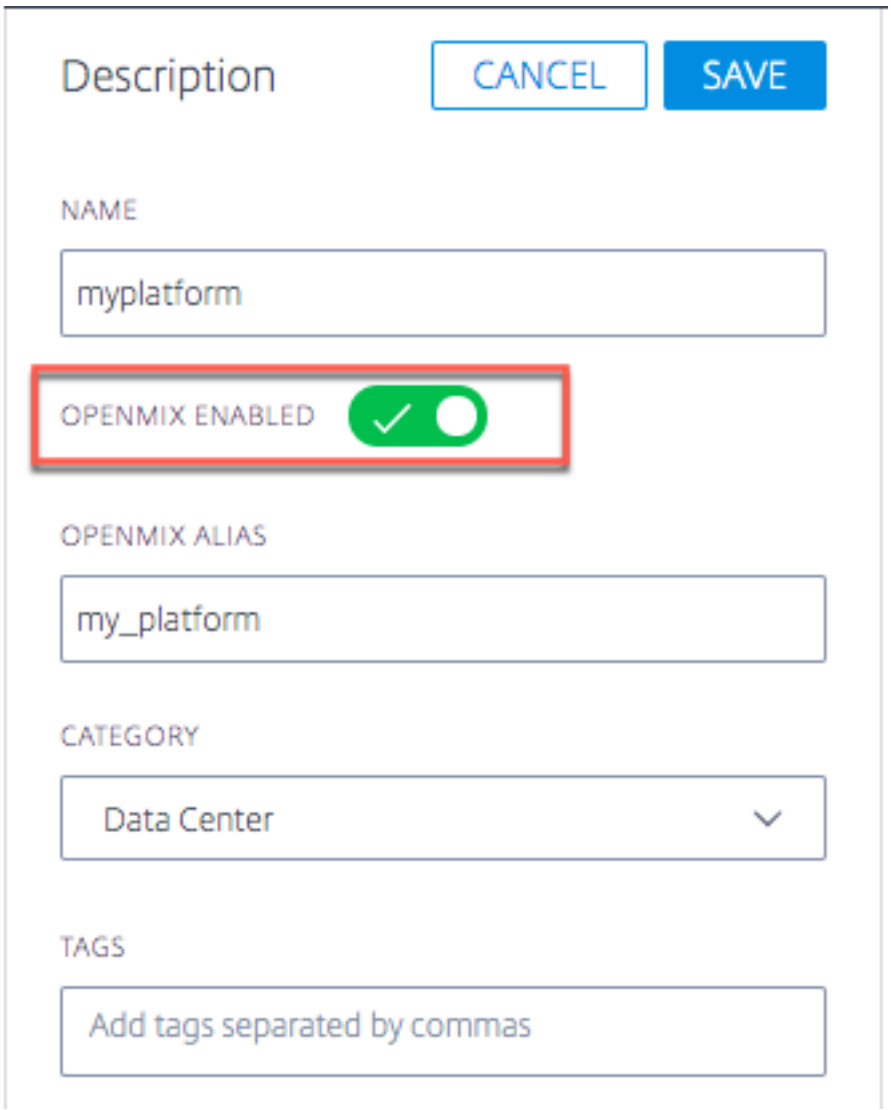


Nota: Si decide volver a cambiar de comunidad a su plataforma privada, tendrá que volver a configurar los ajustes de la sonda de Radar.

Habilitar plataforma para Openmix

Una plataforma se puede activar o desactivar para Openmix activando o desactivando el botón **Openmix Enabled** en **Configuración de plataforma**.

- Haga clic en el **botón Modificar** en **Configuración de la plataforma**
- Seleccione el botón de **Openmix Enabled** para encenderlo.



Si una plataforma en particular está inhabilitada para Openmix, esa plataforma dejará de ser considerada en las decisiones de Openmix. Esto significa que no se generará una puntuación de Radar para esa plataforma en particular.

En las aplicaciones de inicio rápido, la plataforma (si está inhabilitada en la interfaz de usuario) no aparecerá como una opción para ser seleccionada.

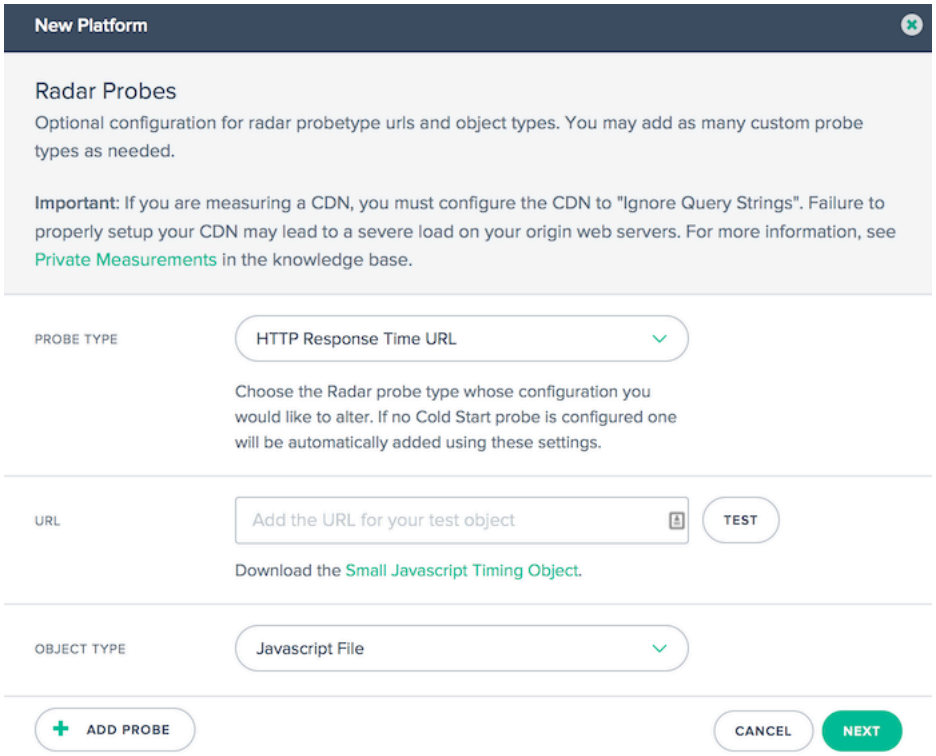
Sin embargo, para las aplicaciones personalizadas, si la plataforma está codificada en la lógica de la aplicación, existe la posibilidad de que se recoja (incluso si esa plataforma está inhabilitada para Openmix en la interfaz de usuario). Para evitar que esto suceda, la aplicación personalizada debe escribirse de tal manera que siempre incluya una lógica para recoger la puntuación de Radar. Cuando la plataforma está inhabilitada para Openmix (en la interfaz de usuario), ya no habrá una puntuación de Radar generada para ella, por lo que la aplicación la ignorará automáticamente.

Esto se puede usar como un interruptor de encendido/apagado operativo si hay un problema con una

plataforma en particular y el cliente quiere sacarlo de todas las aplicaciones durante ese problema.

Configuración de sondas de Radar

Se pueden especificar sondas de Radar para cada plataforma. Por lo general, esto solo es necesario si está configurando una plataforma privada para la supervisión de Radar. Las plataformas públicas proporcionan datos recopilados por la comunidad y se pueden confiar en la mayoría de los usos.



Hay un sondeo para cada tipo de datos recopilados, como: Tiempo de respuesta HTTPS, Rendimiento HTTP, Inicio en frío HTTPS (para disponibilidad), etc. La mayoría de las configuraciones de Radar tienen sondeos para al menos inicio en frío y tiempo de respuesta, con rendimiento en algunos casos.

Cada sondeo tiene los siguientes ajustes:

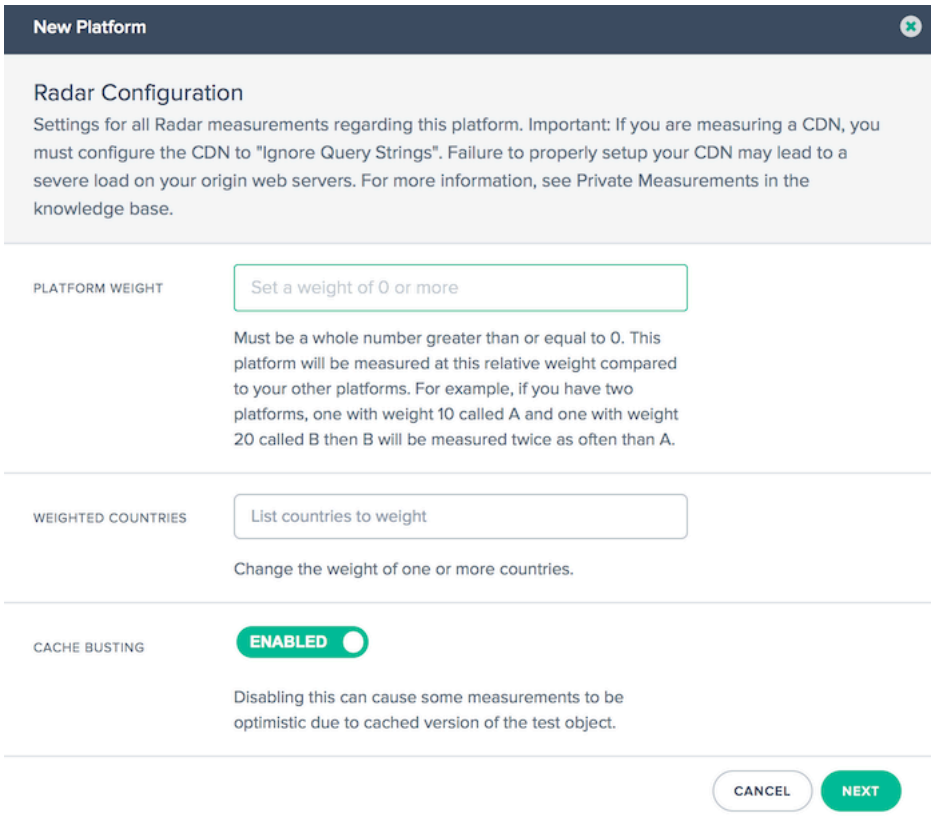
Elemento de entrada	Descripción
Tipo de sonda	Valor para el que se deben comunicar los datos. Existen sondeos separados para cada protocolo (HTTP/HTTPS) y el tipo de datos que se recopilarán (inicio en frío, tiempo de ida y vuelta, rendimiento, etc.).
dirección URL	La dirección URL del objeto de sondeo.

Elemento de entrada	Descripción
Tipo de objeto	El tipo de archivo que se utiliza para tomar la medida. En la mayoría de los casos, desea descargar el “Objeto de sincronización”desde el enlace en el cuadro de diálogo y elegir “Archivo de imagen”. Para los sondeos de servicios DSA, normalmente elegirá “página web (dinámica)”.

Haga clic en **Agregar sonda** en la parte inferior izquierda del cuadro de diálogo y agregue información para cada sondeo. Haga clic en **Guardar** después de introducir todos los sondeos.

Configuración avanzada del Radar

Puede controlar el comportamiento de las comprobaciones de Radar para la plataforma. Estos solo deben cambiarse si comprende el impacto en su aplicación Openmix.



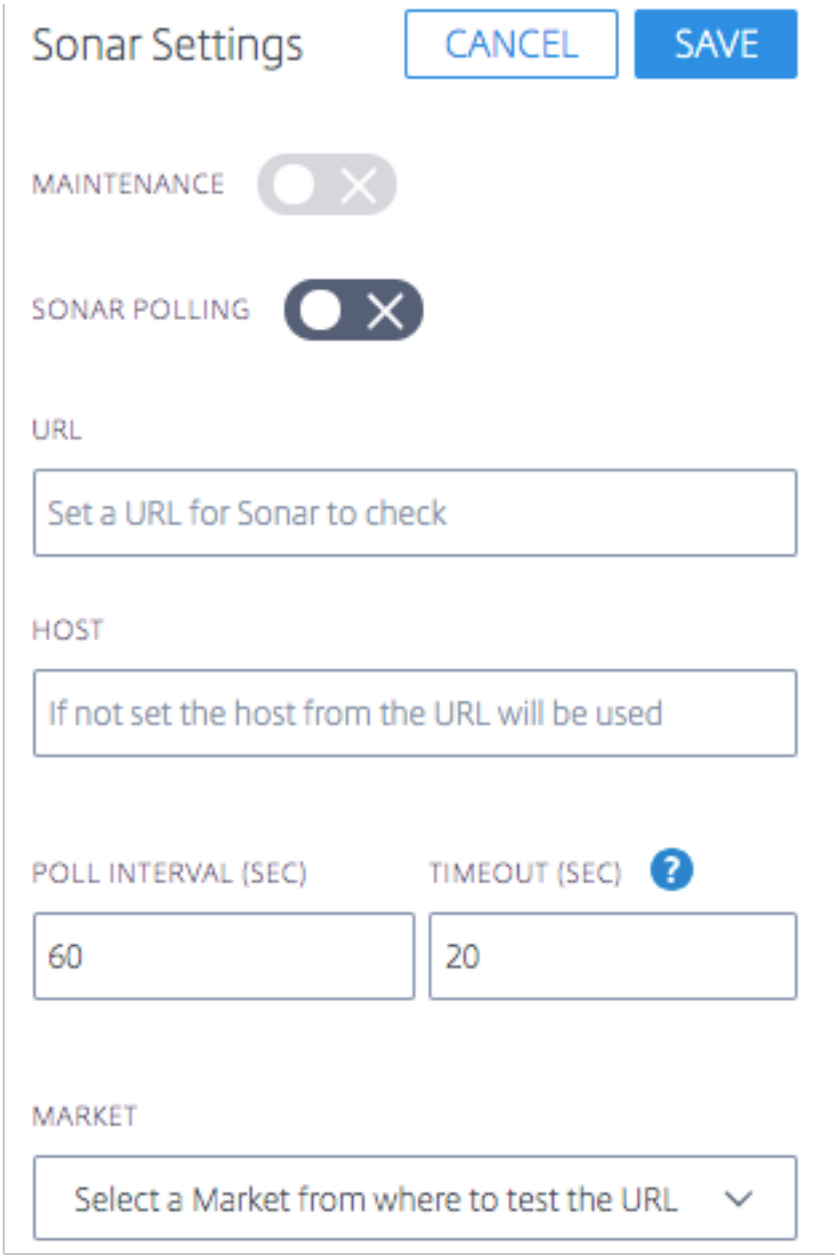
Las siguientes opciones están disponibles:

Elemento de entrada	Descripción	Predeterminado
Peso de la plataforma	Radar utiliza un sistema de ponderación para ayudar a los clientes a priorizar sus pruebas personalizadas, cuanto mayor sea el número mayor será la prioridad de esta prueba privada. Normalmente, esto se usa cuando tiene varias pruebas personalizadas, si está configurando solo una, déjelo como predeterminado.	10, sin ponderación
Países ponderados	Puede anular el peso de la plataforma para determinados países introduciendo los países deseados. El país se especifica mediante los códigos de país ISO.	0, sin ponderación
Peso del país	Si se especifican países ponderados, este peso se aplica a los países y anulará el peso de la plataforma. Si el peso se establece en cero, la plataforma no se medirá en los países especificados.	
Busting de caché	Deshabilitar esta configuración puede provocar que algunas de las mediciones sean optimistas debido a que se informa de versiones almacenadas en caché del objeto de prueba.	Habilitado

Configuración de Sonar

Sonar es un servicio de comprobación de capacidad que se puede utilizar para supervisar la disponibilidad de servicios basados en la web. Sonar funciona realizando solicitudes HTTP o HTTPS desde múltiples puntos de presencia alrededor del mundo a una URL que especifique.

Sonar está habilitado en la configuración de la plataforma. Consulte la guía delSonarusuario para obtener más información.



Plataforma Geo

La plataforma **Geo** es una ubicación (latitud y longitud) asignada a una plataforma. La información geográfica es lo que le permite colocar plataformas con precisión en el mapa en la herramienta **Visualizador**.

Nota: El **Geo**solo se aplica a plataformas que tienen una ubicación física, como centros de datos o regiones en la nube.

Para plataformas privadas

Por defecto no hay ninguna ubicación **geográfica** asignada a las plataformas privadas. Cuando un usuario crea una plataforma privada y configura un sondeo **Radar**, usamos el sondeo para localizarlo geográficamente. Esto significa que cuando agrega una URL a la configuración de **Radar**, localizamos la IP que obtenemos y la asignamos como **Geo** para la plataforma privada. Puede modificar este **Geo** si es necesario. Alternativamente, puede asignar un **Geo** manualmente para su plataforma sin depender de la ruta URL de Radar.

Una vez que el **Geo** está configurado, no se restablece por sí mismo. Incluso si cambia la URL de **Radar**, no cambia el **Geo** de la plataforma. Es necesario modificar el **Geo** manualmente para modificarlo.

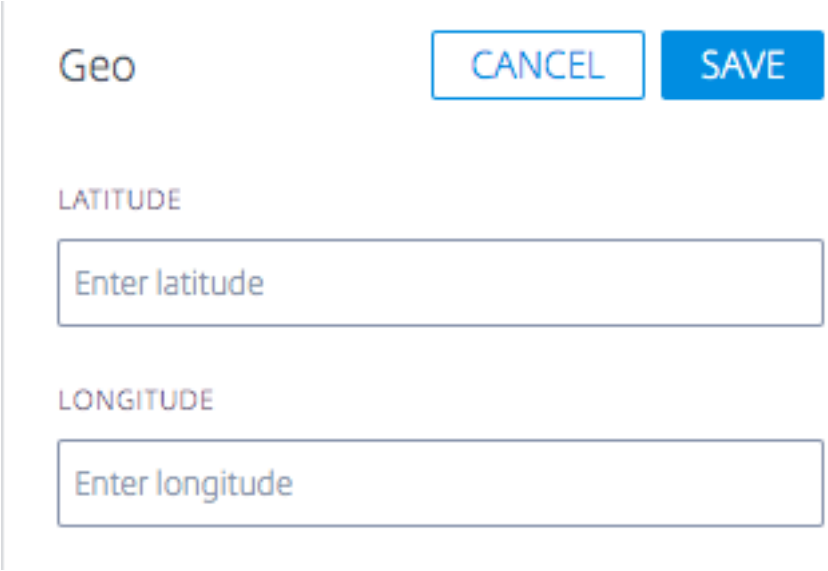
Nota: No todas las plataformas privadas reciben un valor **Geo**asignado. Los geos solo se aplican a plataformas que tienen una ubicación física.

Para plataformas importadas

Si importa una plataforma a través de una configuración GSLB o F5, localizamos la IP pública desde esa configuración y la usamos como el **Geo** de la plataforma.

Para plataformas comunitarias

Cuando un cliente agrega una plataforma comunitaria a su cuenta, de forma predeterminada esta plataforma hereda el geo original de la **Plataforma comunitaria**. Sin embargo, la geografía de esta plataforma puede modificarla el cliente. Normalmente, un cliente no debe tener que modificarlo. Sin embargo, si un cliente elige modificar este **Geo** e introduce una nueva latitud y longitud, la configuración del cliente (para la plataforma de la comunidad) anularía el **Geo** original de la **Plataforma de la Comunidad**.



Openmix

September 13, 2023

Introducción

NetScaler Intelligent Traffic Management (ITM) Openmix ofrece un enfoque revolucionario para la gestión del tráfico global y el equilibrio global de carga de servidores (GTM/GSLB). Para la gestión del tráfico global tradicional, ITM proporciona un enfoque basado en DNS para el equilibrio de carga. ITM utiliza CNAME de DNS o registros en los que las respuestas de DNS se modifican en tiempo real en función de la lógica empresarial requerida. Openmix se puede integrar en el flujo de trabajo y la entrega de vídeo de varias maneras.

Las herramientas y los servicios de GTM o GSLB se basan en motores de reglas estáticos, inextensibles y propietarios para definir y controlar un conjunto limitado de directivas fijas para conmutación por error, operación por turnos y segmentación geográfica. La misión de NetScaler ITM es habilitar estrategias de nube de próxima generación basadas en fuentes de datos en tiempo real. La plataforma Openmix proporciona un medio muy sólido para ingerir datos en tiempo real de varias fuentes. Expone los metadatos como «variables» de entorno que se pueden evaluar en cada solicitud.

Openmix: Principales ventajas

- Elimine las dependencias de un solo proveedor y garantice una disponibilidad del 100%

- Controlar las compensaciones entre precio y rendimiento y eliminar los dolores de cabeza asociados con el abastecimiento múltiple
- Elimine las incertidumbres de las herramientas de rendimiento heredadas y descargue el tráfico de forma selectiva y estratégica
- Aplicar proveedores específicos a mercados específicos

Cómo funciona Openmix

Los clientes inician sesión en Citrix ITM Portal para implementar su primera aplicación. Hay disponible una biblioteca de aplicaciones de ejemplo para comenzar y una herramienta de asistente paso a paso para ayudar a crear aplicaciones con la lógica de redirección más común. Las aplicaciones ITM Openmix pueden admitir dos protocolos para dirigir el tráfico: DNS o HTTP.

Control definido por la aplicación

La plataforma Openmix distribuida a nivel mundial, bajo demanda, mueve la toma de decisiones GTM/GSLB cerca de sus audiencias de aplicaciones. Cada host puede tener su propia aplicación Openmix personalizada que tiene en cuenta las métricas y variables actuales que proporcionan la mejor optimización para cualquier solicitud de enrutamiento.

Los scripts Openmix están programados en JavaScript, un lenguaje accesible para la mayoría de los programadores web y administradores de red. Si bien este enfoque basado en scripts es donde prácticamente cualquier lógica empresarial se puede implementar con una complejidad de codificación mínima para utilizarla como base para directivas de administración de tráfico verdaderamente dinámicas. Gracias a la naturaleza colaborativa de nuestra comunidad de clientes, ITM también proporciona “aplicaciones de inicio rápido”, que son aplicaciones estándar que no requieren código.

Cuándo utilizar los servicios HTTP o DNS

ITM Openmix permite una amplia gama de optimización de la entrega de contenido. El método que use para habilitar Openmix depende en gran medida de los detalles de su caso de uso. El método DNS es fácil de implementar, en su mayoría transparente para los clientes y utilizable en una amplia variedad de contenido. Sin embargo, la capacidad de cambiar de proveedor está limitada por el TTL establecido en la respuesta DNS y parte del contenido no se puede cambiar a un proveedor intermedio diferente. HTTP proporciona más flexibilidad de integración y se pueden tomar decisiones de optimización cuando es óptimo para el cliente. Esa mayor flexibilidad requiere más trabajo para integrarse con un CMS o cliente.

La siguiente tabla resume el caso de uso del cliente para las interfaces DNS y HTTP.

	Openmix DNS	Openmix Web Services (HTTP)
Typical Use	Webpage Optimization Mobile App Optimization Player or Game Download Initial Video/Game Request Mid-Stream Requests (TTL expiration)	Initial Video Request Initial Game Server Selection Mid-Stream Requests Mid-Play Gaming Client Requests
Radar Tag / SDK & Fusion Data Collection	Cedexis Radar RUM CDN & Cloud Performance Monitoring CDN & Cloud Costs data, 3rd Party Monitoring Metrics: Player, Server or App Health, Synthetic Process Monitoring, etc.	
Client Data Collection	Video Player Performance Metrics	
Cedexis Billing	Per Millions of DNS Queries	Per Millions of HTTP Requests

Openmix: DNS

Delegación CNAME La integración más fácil para los clientes de ITM es utilizar la delegación CNAME de DNS. La delegación de CNAME funciona haciendo que el cliente apunte el nombre de host de cara al usuario final (en el siguiente ejemplo `www.acme.com`) a un nombre de host de ITM

```
www.acme.com  600  IN  CNAME  2-02-123d-000d.cdx.cedexis.net.
<!--NeedCopy-->
```

Al recibir una solicitud de DNS de un usuario final, el sistema ITM toma una decisión en tiempo real. La decisión se basa en los datos de Radar, la lógica empresarial de la aplicación y cualquier información de terceros. Esta decisión se articula como otro registro CNAME (en nuestro ejemplo a continuación acme.cdn1.net) o como un registro A como 111.222.111.222.

Al proporcionar un registro CNAME, ITM «dirige» al usuario final a la CDN, la nube o el centro de datos de su elección. Enruta al usuario final para que utilice ese proveedor en lugar de otro.

```
2-02-123d-000d.cdx.cedexis.net.  19  IN  CNAME acme.cdn1.net.
<!--NeedCopy-->
```

Una vez que se suministra la CDN o el CNAME en la nube, la máquina del usuario final continúa con la cadena de resolución. Solicita un servidor de nombres de CDN, hasta que se reciba una dirección IP del nodo o servidor. Donde comienza el proceso de descarga de contenido.
Si se proporciona un registro como parte de la lógica, la máquina del usuario final recibe la dirección IP. Se conecta directamente al servidor e inicia la descarga del contenido.


```
acme.cdn1.net.  132  IN  A  111.222.222.111
<!--NeedCopy-->
```

Delegación de zona Además, la delegación de zona DNS autorizada es una opción para implementar Openmix. El cliente crea una zona DNS y delega en una zona DNS predictiva creada en el portal ITM. Cree un nombre de host en la zona de delegación. Configúrelo para usar una aplicación Openmix o un registro DNS predictivo dinámico para generar una respuesta.
La ventaja de esta opción es que no es necesario que haya una delegación CNAME entre el nombre de host y la respuesta dinámica de la plataforma ITM. Con el ejemplo anterior, `www.acme.com` el nombre de host se resuelve directamente en el valor configurado para la CDN, la nube o el centro de datos óptimos.

```
www.acme.com. 19 IN CNAME acme.cdn1.net.
```

También se pueden usar registros A/AAAA en lugar de CNAME, y el nombre de host se resuelve directamente en el registro del destino óptimo.

```
www.acme.com. 19 IN A 111.222.222.111
```

Implicaciones de DNS y tiempo de vida Factores como los valores de Tiempo de vida (TTL) se consideran cuidadosamente con un tiempo adecuado para el contenido y cómo debe ser la toma de decisiones para los usuarios. En la mayoría de los casos, ITM recomienda un TTL de 20 segundos para el contenido de página y objeto. Para el contenido de vídeo, el consultor de ITM trabaja con el cliente para encontrar el equilibrio más adecuado en función de la longitud del fragmento y el método de integración.

Openmix: HTTP

Una alternativa a DNS es usar la API HTTP. Openmix utiliza solicitudes HTTP para informar a un cliente, como un reproductor de vídeo o CMS, sobre qué plataforma usar en un momento dado.

```
http://hopx.cedexis.com/zones/1/customers/0/apps/1/decision
< HTTP/1.1 200 OK
< Content-Type: application/json
< Date: Mon, 22 Apr 2015 20:25:24 GMT
< Connection: keep-alive
< Content-Length: 177
<
{

  "providers" : [
    {

    "provider" : "cdn2",
```



```
14      "host" : "foo.cdn2.net"
15       }
16   ,
17      {
18
19      "provider" : "cdn1",
20      "host" : "acme.cdn1.net"
21       }
22
23    ]
24   }
25
26 <!--NeedCopy-->
```

El servicio HTTP Openmix utiliza la misma lógica de aplicación que su homólogo basado en DNS. También incluye algunas extensiones adicionales, lo que permite crear más perfiles de una máquina cliente. Por ejemplo, con HTTP Openmix es posible ver los encabezados de User-Agent String, X-Forwarded-For y Referer. Proporcione anulaciones de IP mediante parámetros de cadena de consulta.

Como la carga útil para HTTP Openmix es más extensible que DNS, también es posible proporcionar la selección de decisiones de CDN, nube o servidor de diferentes maneras. El más común hasta ahora ha sido una lista ordenada desde la plataforma más preferida hasta la menos (como arriba). Una lista completa permite que el rango de decisión se proporcione al CMS o al Cliente, pero aun así permite utilizar la heurística interna para elegir el proveedor.

Integración de CMS

Algunos clientes prefieren manejar la selección de proveedores en el lado del servidor en lugar de implementar la selección de proveedores en cada cliente. La API HTTP se puede utilizar para recuperar una decisión de optimización de Openmix en el momento de la solicitud del cliente. Se puede usar para rellenar un archivo que el CMS devuelve al cliente.

De forma predeterminada, los dispositivos de punto final HTTP de Openmix utilizan la IP de la persona que llama para la ubicación geográfica y los criterios de decisión. Si llama desde un CMS u otro sistema que se encuentre entre el cliente del usuario final y Openmix, puede especificar IP como parámetro para usar en la decisión.

```
1 http://hopx.cedexis.com/zones/1/customers/0/apps/1/decision?ip=1.2.3.4
2 < HTTP/1.1 200 OK
3 < Content-Type: application/json
4 < Date: Mon, 22 Apr 2015 20:25:24 GMT
5 < Connection: keep-alive
6 < Content-Length: 177
7 <
8 {
9
```



```
10    "providers" : [
11      {
12
13      "provider" : "cd1",
14      "host" : "acme.cdn1.net"
15       }
16  ,
17      {
18
19      "provider" : "cdn2",
20      "host" : "foo.cdn2.net"
21       }
22
23    ]
24   }
25
26 <!--NeedCopy-->
```

Este método le permite usar una integración de CMS para tomar decisiones de Openmix. También puede obtener los beneficios de la optimización de rutas geográficas e ISP para el usuario final. El nombre de host devuelto por Openmix se empaqueta en la respuesta, como un archivo de manifiesto de vídeo, y el CMS lo devuelve al cliente. El cliente utiliza la decisión optimizada sin necesidad de ninguna modificación para admitir la optimización de Openmix.

Aplicaciones Openmix

Las aplicaciones Openmix Quickstart son aplicaciones de equilibrio de carga y administración del tráfico. Estas aplicaciones proporcionan enrutamiento de tráfico en tiempo real al mejor proveedor en función de un conjunto de reglas.

Las aplicaciones se procesan para cada solicitud realizada a Openmix y se toma una decisión de redirección basada en la lógica especificada. Un cliente puede tener una aplicación para el contenido que tiene un alto valor comercial y una aplicación diferente para el contenido que tiene menos valor. Estas solicitudes se enrutan por separado.

Cuando invoca una aplicación, se envía una sola solicitud a uno de los equilibradores de carga de Citrix. Para DNS, se trata de una única solicitud DNS a los equilibradores de carga DNS. Para HTTP, es una solicitud GET o HEAD al extremo HTTP de Openmix.

Las siguientes aplicaciones están disponibles actualmente a través del portal de administración inteligente del tráfico de NetScaler.

- Redirección estática
- Conmutación por error
- Round Robin
- Tiempo óptimo de ida y vuelta (ORTT)

- Rendimiento
- Proximidad estática

Las aplicaciones JavaScript personalizadas de Openmix son utilizadas por servidores Openmix especializados para responder a solicitudes DNS o HTTP basadas en la lógica de los scripts. La implementación de los scripts se realiza a través del portal del cliente donde se configura y publica la aplicación. Para obtener más información sobre la capacidad de crear sus propios scripts de JavaScript, consulte la información de nuestro intercambio de desarrolladores.

Antes de seguir adelante con la configuración de las aplicaciones, es importante comprender los siguientes conceptos:

Umbral de Disponibilidad

El umbral de disponibilidad es la puntuación de disponibilidad mínima que debe cumplir una plataforma para ser considerada para la redirección. El umbral de disponibilidad mínimo predeterminado para todas las aplicaciones es del 80%. Sin embargo, puede modificar este porcentaje y establecerlo en un valor adecuado para su ubicación, disponibilidad de red y fiabilidad.

Nota: Si ninguna plataforma cumple este umbral de disponibilidad mínimo (el valor predeterminado del 80% o el valor que ha establecido), la redirección aleatoria se realiza para las aplicaciones Round Robin, ORTT y Rendimiento.

Retroceso

La respuesta de reserva se devuelve si la aplicación Openmix no se ejecuta correctamente por cualquier motivo. O si Sonar confirma que no hay plataformas disponibles. Por lo tanto, se debe especificar un registro CNAME/A/AAAA de reserva válido o IP (o ruta en HTTP) con el que Openmix puede responder. Esta URL alternativa o registro CNAME puede ser para una plataforma que esté preconfigurada en Openmix.A veces, la
reserva se produce durante los siguientes escenarios también:

- Al cambiar entre versiones de la aplicación, carga y publica un nuevo script. Hay un breve período de tiempo de reserva de milisegundos hasta que se inicialice el nuevo script y se elimine el anterior.
- Si alguna vez se produce una sobrecarga (lo que rara vez ocurre), Openmix responde con el CNAME/A/AAAA de reserva, ya que el retroceso compensa la carga en el servicio.

Como alternativa, debe introducir un nombre de host válido (registro CNAME/A/AAAA) o una dirección IP en el DNS, y un URI válido (puede tener el formato `scheme:[//host[:port]][/path][?query][#fragment])` en HTTP.

TTL

En Openmix, el DNS Time to Live (TTL) de la aplicación indica a los solucionadores cuánto tiempo deben mantener la decisión antes de volver a preguntar a Openmix.
El TTL se usa para controlar el volumen de tráfico que recibe una aplicación Openmix. También controla qué tan sensible debe ser una aplicación a los cambios en los datos sobre los que actúa.
El TTL predeterminado es 20 segundos. Aunque puede modificar este valor, no se recomienda hacerlo. Si baja el TTL, obtiene más volumen y más consultas DNS en tiempo real. Puede generar costes adicionales y un menor rendimiento porque las consultas de DNS llevan tiempo en el cliente. Por lo tanto, es mejor no cambiar el valor predeterminado de TTL.

> **Nota:** El Tiempo de vida se aplica a las aplicaciones de inicio rápido, a las aplicaciones JS personalizadas si no se especifica ningún TTL en el código y a todas las respuestas de reserva

Pesos (Utilizados para Round Robin)

Puede asignar pesos para la priorización y selección de cada plataforma a nivel mundial y/o por mercado o país.

Por ejemplo, supongamos que tiene tres plataformas seleccionadas para su aplicación: P1, P2 y P3. Les das los pesos: 60, 50 y 10 respectivamente. La aplicación Round Robin convierte estos valores en porcentajes como P1 = 50%, P2 = 42% y P3 = 8%, lo que suma un 100%. Estos porcentajes significan que el 50% de las veces, los usuarios son enrutados a través de P1, el 42% del tiempo a través de P2 y el 8% del tiempo a través de P3.

Los pesos que le das a las plataformas no tienen que sumar hasta 100. Pueden ser cualquier entero entre 0 y 1 000 000. Los pesos que se dan a las plataformas cuando se convierten en porcentajes (por la aplicación en el back-end), suman un 100%. Si todas las plataformas seleccionadas reciben el mismo peso, el tráfico se distribuirá uniformemente entre ellas a lo largo del tiempo. Si tienes una plataforma, entonces esa plataforma se usa el 100% del tiempo, independientemente del peso que le des.

Los pesos solo se utilizan para plataformas que se consideran disponibles según las comprobaciones de disponibilidad de Radar y Sonar, dependiendo de la configuración de la aplicación. Las plataformas no disponibles hacen que la distribución no coincida con los pesos configurados. Por ejemplo, si P1 pesa 100 y P2 pesa 0, pero P1 no pasa la comprobación de disponibilidad del radar, todo el tráfico pasa a P2.

Hándicap (utilizado para ORTT y rendimiento)

El **Hándicap** es un valor porcentual que se puede aplicar a una plataforma para modificar las puntuaciones del Radar para RTT y el rendimiento es decir, aumentar artificialmente el tiempo de respuesta

(en milisegundos) o disminuir el rendimiento (en kbps). Aumentar o disminuir estos valores reduce el rendimiento de la plataforma, de modo que la probabilidad de que se recoja sea baja. Los hándicaps se pueden agregar a las plataformas a nivel mundial o por separado para mercados o países específicos.
En los casos en que una plataforma es cara en un mercado o país específico y desea reducir su probabilidad de ser elegida cuando un proveedor equivalente está cerca en términos de rendimiento. Pones un valor de hándicap como multiplicador para aumentar el valor del tiempo de respuesta o disminuir el valor del rendimiento. Como resultado, reduce la probabilidad de que se elija una plataforma.

A continuación se muestra cómo funciona **Hándicap** en el backend:

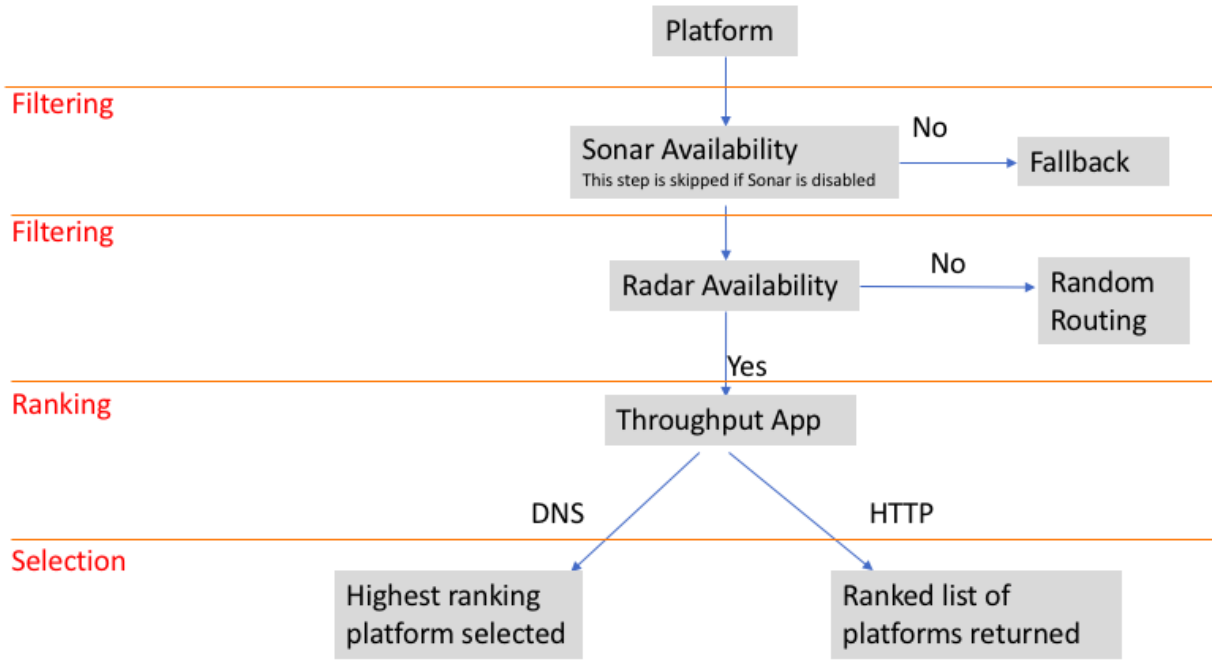
- RTT de plataforma con Hándicap aplicado = RTT (tiempo de ida y vuelta en milisegundos) * (1 + Hándicap) o
- Rendimiento de plataforma con Hándicap aplicado = (Rendimiento en kbps) * (1 —Hándicap)

Nota: Los valores RTT y Rendimiento de la plataforma son puntuaciones de los datos de Radar.
La siguiente tabla muestra cómo Hándicap afecta a las dos plataformas: P1 y P2. Y cómo el Hándicap disminuye la probabilidad de que P1 sea elegido.

	P1	P2
RTT sin Hándicap	50 milisegundos	60 milisegundos
RTT con 50% (0.5) Hándicap para P1 y 0% (0) para P2	50 (1+0,5) = 75 milisegundos	60 (1+0) = 60 milisegundos
Rendimiento sin hándicap	3000 kbps	2800 kbps
Rendimiento con 50% (0.5) Hándicap para P1 y 0% (0) para P2	3000 (1-0.5) = 1500 kbps	2800 (1- 0) = 2800 kbps

Flujo de trabajo de filtrado, clasificación y selección

Diagrama de flujo de ejemplo para la aplicación de rendimiento



Criterios de selección de plataformas

Las aplicaciones Openmix Quickstart utilizan los siguientes criterios como filtros de primer, segundo y tercer nivel para clasificar y seleccionar la mejor plataforma.

Nivel de filtración	Criterios de selección	ORTT	Rendimiento	Round Robin	Conmutación por error	Redirección estática	Proximidad estática
1.º nivel	Comprobación de disponibilidad de Sonar (si está activado)	X	X	X	X	X	X

Nivel de filtración	Criterios de selección	ORTT	Rendimiento	Round Robin	Conmutación por error	Redirección estática	Proximidad estática
2.º nivel	Comprobación de disponibilidad del Radar (si está activado)	X	X	X	X	X	NA
3.º nivel	Pesos (definidos por el usuario)	NA	NA	X	NA	NA	NA
3.º nivel	Tiempo de ida y vuelta (en milisegundos)	X	NA	NA	NA	NA	NA
3.º nivel	Rendimiento (en kbps)	NA	X	NA	NA	NA	NA

Informes de código de motivo

Los códigos de motivo proporcionan visibilidad de por qué se tomó la decisión y también permiten saber qué parte del código de la aplicación se ejecuta. Durante la ejecución, una aplicación puede agregar algo al campo de código de motivo en cualquier momento.Los códigos de motivo significan cosas diferentes para cada aplicación de inicio rápido. Hay algunos puntos en común entre los códigos de motivo de cada aplicación, pero no es exhaustiva.

Nota: Para que los códigos de motivo se muestren correctamente, no deben exceder el límite máximo de 200 caracteres. Si se supera este límite, el código de motivo se muestra como **Desconocido**. Si el usuario no ha agregado un código de motivo, se mostrará **Desconocido**.

Los siguientes son los códigos de motivo para las aplicaciones de inicio rápido:

Código de motivo	Descripción	RTT óptimo	Round Robin	Redirección estática	Rendimiento	Proximidad estática	Conmutación por error
Disponibilidad óptima	El proveedor con mejor rendimiento está disponible y ha sido seleccionado.	X	N/D	N/D	X	N/D	X
No disponibilidad óptima: Radar	El proveedor con mejor rendimiento no está disponible; se ha seleccionado otro proveedor elegible que está disponible según el radar	X	N/D	N/D	X	N/D	X
No disponibilidad óptima: Radar y sónar	El proveedor con mejor rendimiento no está disponible debido a un radar o un sónar.	X	N/D	N/D	X	N/D	X

Código de motivo	Descripción	RTT óptimo	Round Robin	Redirección estática	Rendimiento	Proximidad estática	Conmutación por error
Ninguna disponibilidad: Radar	Según el radar, todas las plataformas elegibles no están disponibles. Solicitud dirigida a una opción de reserva	X	X	N/D	X	N/D	X
Ninguna disponibilidad: Sónar	Según el sónar, todas las plataformas elegibles no están disponibles. La solicitud se ha enviado a una opción de reserva.	X	X	N/D	X	N/D	X

Código de motivo	Descripción	RTT óptimo	Round Robin	Redirección estática	Rendimiento	Proximidad estática	Conmutación por error
Problema de datos	Indica las mediciones de radar que faltan para una o más plataformas. Como resultado, la plataforma se elige al azar.	X	X	N/D	X	N/D	X
Valor predeterminado geográfico	La configuración geográfica predeterminada está en vigor.	X	X	N/D	X	X	X
País de superditación geográfica	Está en vigor una superditación por país para esta decisión	X	X	N/D	X	X	X
Mercado de superditación geográfica	Está en vigor una superditación de mercado para esta decisión	X	X	N/D	X	X	X

Código de motivo	Descripción	RTT óptimo	Round Robin	Redirección estática	Rendimiento	Proximidad estática	Conmutación por error
Toda la disponibilidad	Todas las plataformas elegibles están disponibles a través de sónar y radar	X	X	N/D	X	N/D	N/D
Disponibilidad próxima	La plataforma geográfica más cercana está disponible y ha sido seleccionada	X	N/D	N/D	N/D	X	N/D
No disponibilidad elegible: Radar	Para Round Robin, el proveedor elegible no está disponible según el radar	N/D	X	N/D	N/D	N/D	N/D

Código de motivo	Descripción	RTT óptimo	Round Robin	Redirección estática	Rendimiento	Proximidad estática	Conmutación por error
Aplicación persistente	La decisión sirvió como respuesta en caché, no se ejecutó ninguna lógica	X	X	X	X	X	X
Solicitud geográfica no disponible	No se puede establecer la ubicación geográfica de la solicitud. Solicitud dirigida a una opción de reserva	X	N/D	N/D	N/D	X	N/D
Ninguna disponibilidad: Proveedor	Todos los proveedores no están disponibles. Solicitud dirigida a una opción de reserva	X	N/D	N/D	N/D	X	N/D

Código de motivo	Descripción	RTT óptimo	Round Robin	Redirección estática	Rendimiento	Proximidad estática	Conmutación por error
No disponibilidad: Proveedor: Distancia	No se han encontrado puntuaciones de proximidad para ningún proveedor. Solicitud dirigida a una opción de reserva	X	N/D	N/D	N/D	X	N/D

Aplicaciones Openmix Quickstart

1. Inicie sesión en el portal de administración inteligente del tráfico de NetScaler.
2. En el menú de navegación de la izquierda, vaya a **Openmix > Configuración de la aplicación**.
3. Si está configurando su aplicación Openmix por primera vez, verá la página **Introducción** al hacer clic en **Openmix > Configuración de la aplicación**.
4. Para configurar una nueva aplicación, haz clic en el botón **Empezar** o en el botón **Agregar** en la esquina superior derecha de la página. Si las aplicaciones Openmix se han configurado previamente, verá una lista de aplicaciones en esta página.

Las siguientes secciones le guían a través del proceso de configuración de aplicaciones Openmix en el portal.

Redirección estática

Este tipo de aplicación no utiliza ninguna lógica de evaluación para decidir qué respuesta DNS debe proporcionarse al usuario final. La aplicación siempre selecciona una única plataforma aquí, especificada por el usuario. Por lo tanto, la aplicación usa solo una respuesta DNS CNAME o dirección IP. La aplicación de enrutamiento estático se puede configurar a través del portal en la página **Configuración de la aplicación** .

Nota: Antes de configurar la aplicación, asegúrese de que las plataformas estén configuradas primero. Consulte la página Plataformas para obtener información sobre la configuración

Navegación

1. Vaya a **Openmix > Configuración de la aplicación**.
2. Haga clic en el botón **Agregar** en la parte superior derecha

Se abrirá el cuadro de diálogo **Información básica**.

Información básica Siga estos pasos para introducir **información básica**:

1. Para **Protocolo**, seleccione DNS o HTTP de la lista.
2. En **Tipo de aplicación**, seleccione Redirección estática. O si está configurando otro tipo de aplicación, selecciónela de la lista.
3. Asigne un **nombre** a su aplicación (campo obligatorio), agregue una **descripción** (campo opcional) y una **etiqueta** (campo opcional).
4. Haga clic en **Siguiente** para **Configuración**.

Configuración Para configurar la aplicación, haga lo siguiente:

1. Seleccione la plataforma asociada en la lista **Plataforma**. Es la plataforma que configura en la página Plataformas, que representa la CDN, la nube o el centro de datos.
2. Introduzca un registro **CNAME/A/AAAA** (para DNS) o **URL** (para HTTP). El CNAME DNS o la URL HTTP de la plataforma seleccionada debe apuntar a una dirección IP o un nombre de host válidos.
3. Para **CORS**, en un protocolo HTTP, seleccione Ninguno, Todo o Personalizado para CORS. CORS le permite controlar el acceso a su sitio desde otros sitios. Puede restringir completamente el acceso a su sitio desde otros sitios (haciendo clic en **Ninguno**), permitir el acceso desde todos los demás sitios (haciendo clic en **Todos**) o permitir el acceso solo desde sitios específicos (haciendo clic en **Personalizar**).
4. Introduzca un **TTL** (tiempo de vida) para la respuesta. El valor predeterminado es 20 segundos, pero se puede anular.
5. Haga clic en **Completar**.
6. En la ventana emergente de confirmación, haga clic en **Listo** o **Publicar** para ver su aplicación en la página de aplicaciones de Openmix. Si hace clic en **Publicar**, la aplicación se activa al instante y tiene un estado verde. Significa que la aplicación está en producción. Si haces clic en **Listo**, la aplicación seguirá apareciendo en la página de aplicaciones, pero no se ha publicado y el estado es rojo.

Conmutación por error

La aplicación Conmutación por error admite una lógica de redirección simple en la que se elige una plataforma en función de su lugar en línea y de su disponibilidad. El cliente puede crear una cadena de conmutación por error que decida qué plataforma seleccionar primero, segundo, etc. Esta cadena de conmutación por error se puede crear para funcionar a nivel mundial o para mercados y países individuales.

La aplicación de **conmutación por error** se puede configurar dentro del portal en la página **Configuración de la aplicación**.

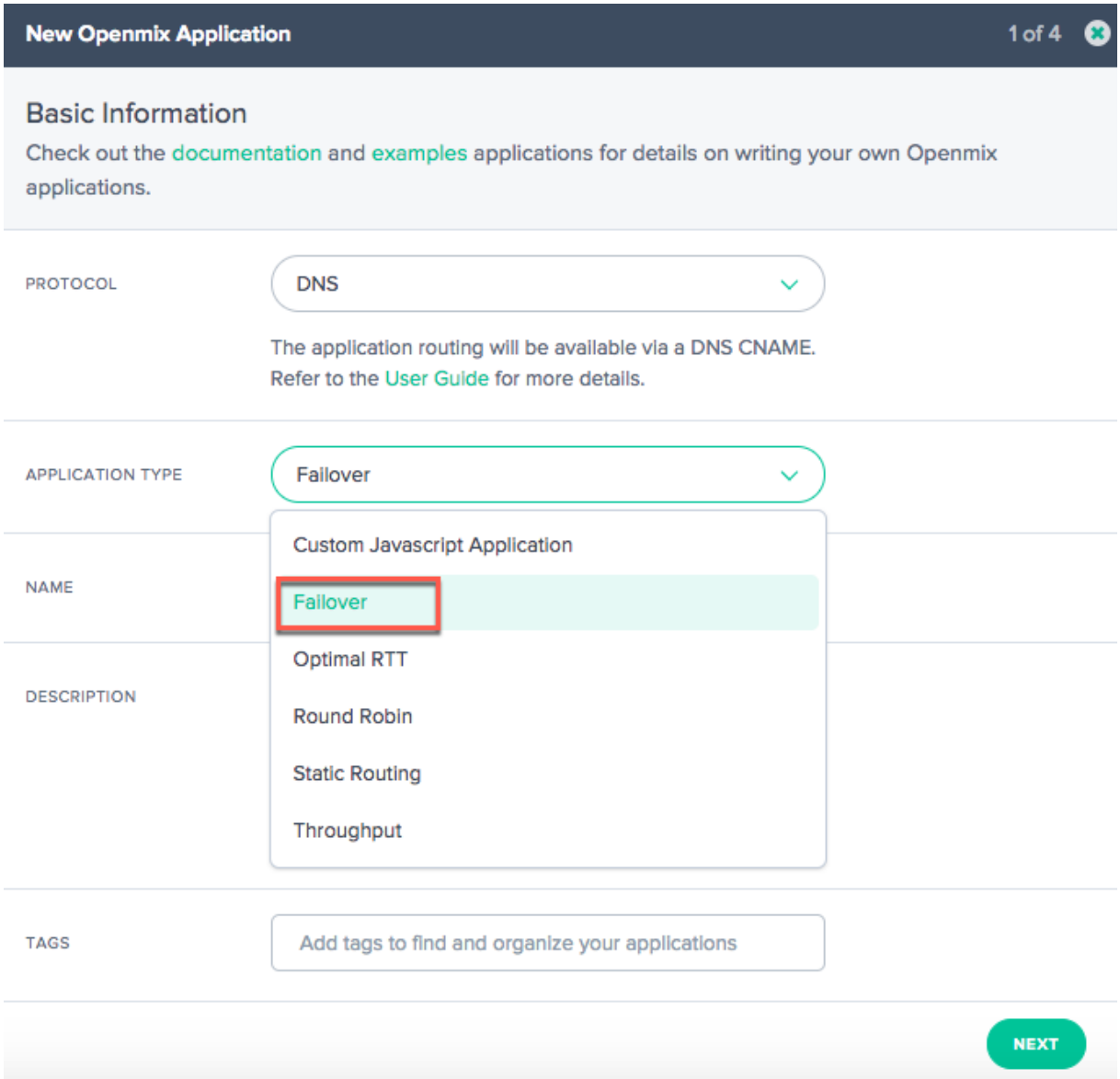
Nota: Antes de configurar la aplicación, asegúrese de que las plataformas estén configuradas primero. Consulte la página Plataformas para ver la configuración de la plataforma.

Navegación

1. Inicie sesión en el Portal.
2. En el menú de navegación de la izquierda, vaya a **Openmix > Configuración de la aplicación**.
3. Haga clic en el botón Agregar en la parte superior derecha para acceder al cuadro de diálogo Nueva aplicación Openmix, **Información básica**.

Información básica

1. Seleccione **DNS** en la lista **Protocolo**.
2. En la lista **Tipo de aplicación**, seleccione **Conmutación por error**.
3. Asigne un **nombre** (campo obligatorio) a su aplicación, agregue una **descripción** (campo opcional) y una **etiqueta** (campo opcional).
4. Cuando haya terminado, haga clic en **Siguiente**.



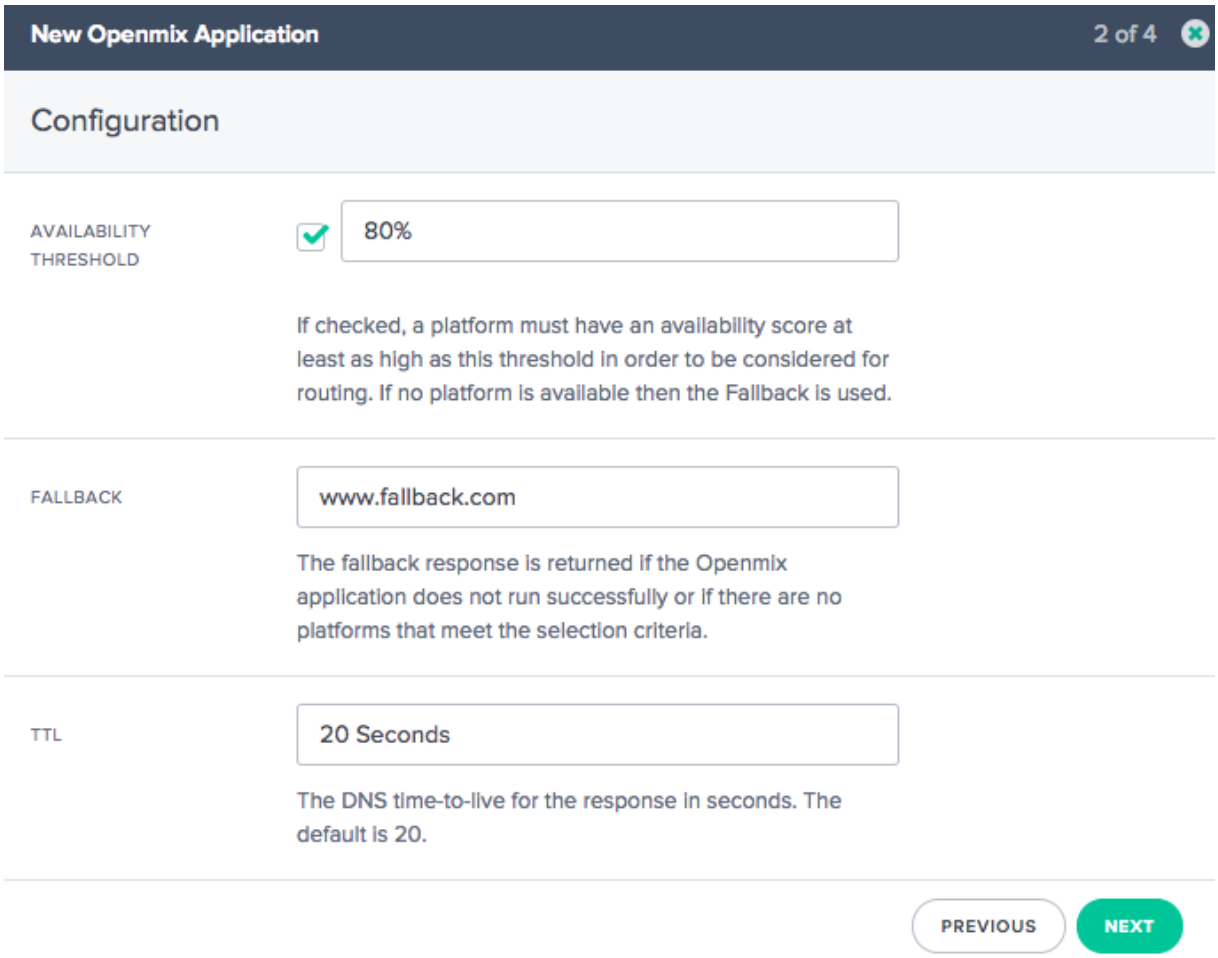
Configuración

1. En el cuadro de diálogo Configuración, active la casilla **Umbral de disponibilidad**. El umbral de disponibilidad tiene un valor predeterminado del 80%. Una plataforma debe tener una puntuación de disponibilidad al menos tan alta como este umbral para que se tenga en cuenta para el enrutamiento.

    - Si quiere modificar el umbral de disponibilidad predeterminado, simplemente escriba un nuevo valor para reemplazar el valor predeterminado.
    - Si ninguna plataforma tiene una puntuación de disponibilidad igual o superior al umbral especificado, se utiliza la dirección CNAME o A o AAAA o IP de reserva.
    - Si la casilla de verificación no está seleccionada, la plataforma asume un umbral de

disponibilidad cero. Significa que no hay verificación de disponibilidad de Radar en esta plataforma.

2. Introduzca un CNAME/A/AAAA o una dirección IP para **Fallback**. Normalmente, el CNAME/A/AAAA o IP de reserva se utiliza si la aplicación encuentra problemas o errores.
3. Introduzca un **TTL** (tiempo de vida) para la respuesta. El valor predeterminado es de 20 segundos. Puede anular este valor si es necesario.



Información de la plataforma

1. En el cuadro de diálogo **Información de plataforma**, seleccione una **plataforma** de la lista.

   - Puede seleccionar varias plataformas mediante el botón **Agregar plataformas**. La idea es seleccionar todas las plataformas disponibles aplicables para la redirección global y geográfica (mercados y países).
   - Las plataformas de esta lista son las que configura en la página Plataformas del portal, que representan su CDN, la nube o el centro de datos.
   - Todas las aplicaciones Openmix requieren que se configure previamente una plataforma

asociada. Si no encuentra una plataforma en la lista, puede configurarla en la página Plataformas del portal.

2. Introduzca el registro **CNAME/A/AAAA** para la plataforma.
3. Asegúrese de que la casilla **Habilitado** está activada (lo que indica que la plataforma está habilitada) antes de pasar al siguiente paso.
4. Si **Sonar** está configurado y desea usar los datos de Sonar para ayudar en el proceso inicial de toma de decisiones, asegúrese de hacer clic en la casilla **Usar Sonar para la disponibilidad de la plataforma** . **Nota**: La casilla de verificación Sonar solo aparece si Sonar está habilitado para esa plataforma.
5. Haga clic en **Siguiente** para **Configuración de ubicación**.

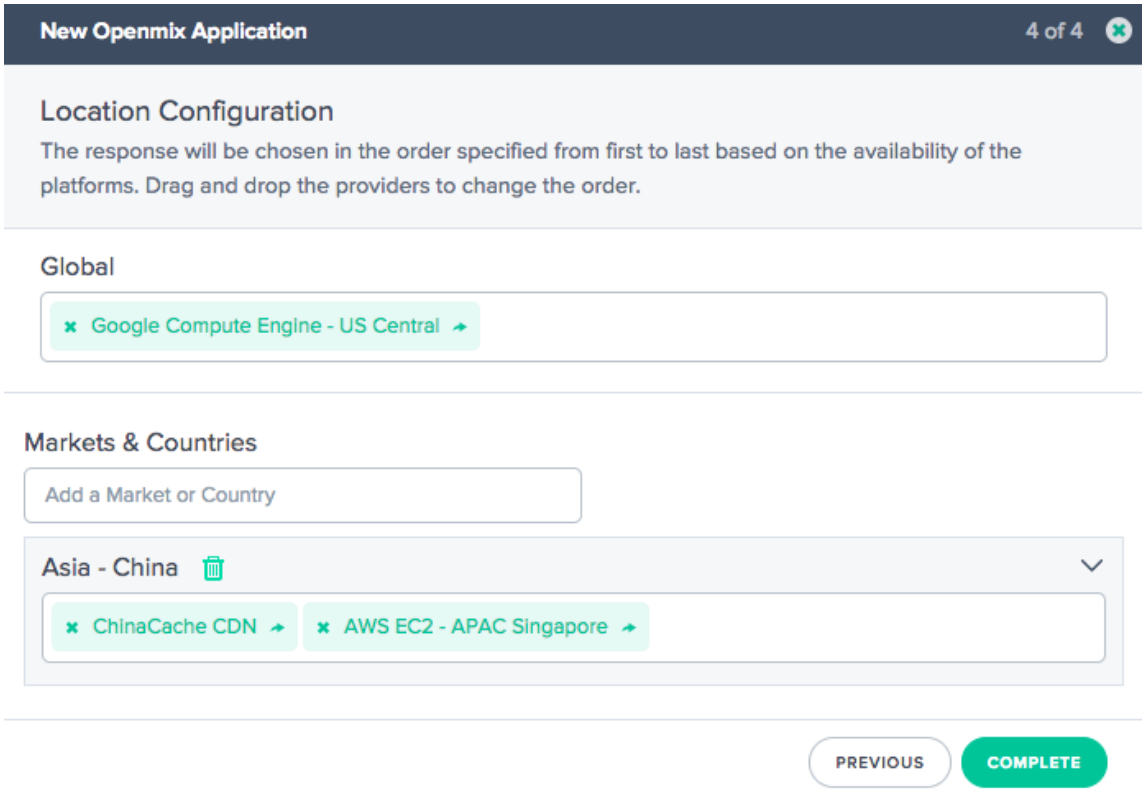
Configuración de ubicación

1. En el cuadro de diálogo **Configuración de ubicación**, seleccione las plataformas necesarias para Redirección **global**.

   - **Global** indica que está configurando una cadena de plataformas para la redirección global.
   - Al hacer clic dentro del campo **Global**, una lista muestra todas las plataformas seleccionadas en el paso **Información de plataforma**.
   - Seleccione las plataformas necesarias de la lista para la redirección global basada en disponibilidad.
   - El orden en el que coloque los nombres de las plataformas en este campo determinará la prioridad de su selección. Por ejemplo, si la primera plataforma de la lista no está disponible, se selecciona la segunda. Si ninguna de las plataformas de la lista está disponible, entonces se utiliza el respaldo.
   - Puede arrastrar los nombres de la plataforma para cambiar su orden de prioridad.

2. Haga clic en **Mercados y países** si quiere configurar plataformas para la redirección geográfica local.

   - Al hacer clic dentro del campo **Mercados y países**, la lista muestra todas las plataformas seleccionadas en el paso **Información de la plataforma**.
   - Seleccione plataformas para la redirección geográfica local, por separado para cada geografía (mercado/país).
   - El orden en el que coloque los nombres de las plataformas en este campo determinará la prioridad de su selección. Por ejemplo, en China, desea usar primero el POP de China, y solo si no está disponible, querrá que se use su POP de Singapur, que colocaría a continuación en la línea, y así sucesivamente.
   - Puede arrastrar los nombres de la plataforma para cambiar su orden de prioridad.



3. Haga clic en **Completar**para terminar de configurar la aplicación.
4. En la ventana emergente de confirmación, haga clic en **Listo** o **Publicar** para ver su aplicación en la página de **Openmix**.
   - Si hace clic en **Publicar**, la aplicación se activa al instante y tiene un estado verde. Su aplicación está en producción.
   - Si **hace clic en Listo**, la aplicación seguirá apareciendo en la página de Openmix, pero no se ha publicado y el estado es rojo.

Round Robin

Esta aplicación sigue una metodología típica de equilibrio de carga de servidor global de Round Robin, donde cada CNAME alterna se devuelve a los usuarios finales, a medida que se realizan las solicitudes DNS. Utiliza datos de Sonar (si Sonar está habilitado) y el umbral de **disponibilidad de la plataforma** para evaluar la mejor plataforma para el usuario solicitante. Cada plataforma se selecciona en función de la metodología de distribución Round Robin. Por ejemplo, si las plataformas P1, P2 y P3 cumplen con el umbral de disponibilidad, la primera solicitud se enruta a P1, la segunda a P2 y la tercera a P3. La cuarta solicitud se enruta nuevamente a P1, y así sucesivamente.

Para configurar una nueva aplicación Round Robin, haz clic en el botón **Agregar** en la esquina superior derecha de la página Openmix. Se abre el cuadro de diálogo **Información básica**.

Navegación

1. Inicie sesión en el Portal.
2. En el menú de navegación de la izquierda, vaya a Openmix > Configuración de la aplicación.
3. Haga clic en el botón Agregar en la parte superior derecha para acceder al cuadro de diálogo Nueva aplicación Openmix, Información básica.

Información básica

1. En el cuadro de diálogo Información básica, seleccione DNS como Protocolo para Round Robin.**Nota**: Para la aplicación Round Robin, la redirección solo está disponible a través de un CNAME DNS.
2. Seleccione el **tipo de aplicación** de la lista. Asigne a la aplicación un **nombre** (campo obligatorio), una **descripción** (campo opcional) y una **etiqueta** (campo opcional).
3. Haga clic en **Siguiente** para configurar.

Configuración

1. El **umbral de disponibilidad** tiene un valor predeterminado del 80%. Para modificar este valor, simplemente escriba un nuevo valor para reemplazar el valor predeterminado.
2. Introduzca un CNAME/A/AAAA o una dirección IP para Fallback. Normalmente, el CNAME/A/AAAA o IP de reserva se utiliza si la aplicación encuentra problemas o errores.
3. Introduzca un TTL (tiempo de vida) para la respuesta. El valor predeterminado es 20 segundos, pero este valor se puede anular si es necesario.
4. Haga clic en **Siguiente** para obtener información sobre la plataforma.

Información de la plataforma

1. Seleccione una plataforma de la lista **Plataforma**. **Nota**: Todas las aplicaciones Openmix requieren una plataforma asociada configurada previamente. Si no encuentra una plataforma en la lista, puede configurarla en la página Plataformas del portal.
2. Seleccione más plataformas haciendo clic en el botón **Agregar plataforma**.
3. Introduzca un CNAME o un registro A/AAAA o IP (en DNS), o URL (en HTTP) para esta plataforma. Debe ser una dirección URL, un nombre de host o una dirección IP válidos. Puede tener el formato: `scheme:[//host[:port]][/path][?query][#fragment]`.
4. Asegúrese de que la casilla **Habilitado** está activada (lo que indica que la plataforma está habilitada) antes de pasar al siguiente paso.
5. Si Sonar está disponible y desea usar los datos de Sonar para ayudar en el proceso inicial de toma de decisiones, asegúrese de hacer clic en la casilla **Usar Sonar para la disponibilidad de la plataforma** .
6. Haga clic en **Guardar** para ir al paso 4 y asignar los pesos adecuados para cada plataforma.

Configuración de ubicación

1. Asignar **pesos** para la priorización y selección de cada plataforma a nivel mundial y/o por mercado o país.
2. Para asignar pesos de plataforma por separado para el mercado o el país, introduzca el nombre en el cuadro de búsqueda Mercados y países y elija de la lista.
3. Haga clic en **Completar** para crear la aplicación.
4. En la ventana emergente de confirmación, haz clic en **Listo** o **Publicar** para ver tu aplicación en la página de Openmix. Si hace clic en **Publicar**, la aplicación se activa al instante y tiene un estado verde. Su aplicación está en producción. Si **hace clic en Listo**, la aplicación seguirá apareciendo en la página de Openmix, pero no se ha publicado y su estado es rojo.

Aplicación de tiempo óptimo de ida y vuelta (ORTT)

La aplicación ORTT utiliza el tiempo de respuesta del radar, los datos del sonar, si Sonar está activado, y el umbral de disponibilidad de la plataforma para evaluar la mejor plataforma para el usuario que lo solicita. El umbral de disponibilidad es la disponibilidad mínima (80% es el valor predeterminado) que la plataforma debe cumplir para ser seleccionada. Además, la aplicación ORTT también utiliza un valor de Hándicap que, a nivel mundial o local, permite a los clientes influir en cómo enrutar a los usuarios finales.

Los tres primeros pasos: Información básica, Configuración e Información de plataforma, se introducen de la misma manera que las demás aplicaciones.

Siga estos pasos para configurar la información de ubicación e introduzca valores para **Hándicap** para cada plataforma, globalmente, o por ubicación/mercado.

Configuración de ubicación

1. En el cuadro de diálogo **Configuración de ubicación**, introduzca un valor para **Hándicap** para una o todas las plataformas seleccionadas. Puede introducir un valor de hándicap entre 0 y 6000. El uso del hándicap es reducir manualmente las posibilidades de que se elija una plataforma en particular para la redirección, cuando hay mejores plataformas disponibles, en términos de coste o conveniencia. Cuanto mayor sea el valor del hándicap, menor será la probabilidad de que se escoja la plataforma. Si es necesario, puede anular la selección de una plataforma desactivando el botón **Selección de plataforma**.
2. Haga clic en **Mercados y países** para seleccionar un mercado o país concreto de la lista e introduzca los valores de **Hándicap** por separado para cada una de las plataformas asociadas.
3. Haga clic en **Completar**para terminar de configurar la aplicación.
4. En la ventana emergente de confirmación, haga clic en **Listo** o **Publicar** para ver su aplicación en la página de lista de aplicaciones de Openmix. Si hace clic en **Publicar**, la aplicación se activa

al instante y tiene un estado verde. Su aplicación está en producción. Si **hace clic en Listo**, la aplicación seguirá apareciendo en la página Aplicaciones, pero no se ha publicado y su estado es rojo.

Rendimiento

La aplicación **Rendimiento** selecciona la plataforma en función de los datos de Sonar (si Sonar está habilitado), el rendimiento más alto (utilizando datos de Radar) y el umbral de disponibilidad de la plataforma (que es del 80% de forma predeterminada). Además, esta aplicación le permite agregar un valor de Hándicap para disminuir el rendimiento de plataformas específicas e influir en cómo se redirigen los usuarios finales. Este valor opcional de Hándicap se puede asignar global y/o localmente (para mercados o países específicos).

Los tres primeros pasos (**Información básica, Configuración e Información de plataforma**) se introduzcan de la misma manera que las otras aplicaciones. La **configuración de ubicación** se introduce de la misma manera que en la aplicación ORTT.

Cuando haya terminado, haga clic en **Completar** para volver a la página de lista de aplicaciones Openmix. Por último, haga clic en **Publicar** para publicar la aplicación cuando esté listo para comenzar a funcionar.

Estado de la solicitud

El estado de la aplicación muestra su configuración actual.

- Rojo significa inédito. Cuando complete la configuración, si **hace clic en Listo**, la aplicación aparecerá en la página de aplicaciones con un punto rojo, lo que indica que aún no se ha publicado.
- Verde significa "publicado". Si hace clic en **Publicar**, su aplicación se activa instantáneamente y se indica con un punto verde, lo que significa que la aplicación está en producción.
- El amarillo significa la versión más reciente que no se ha publicado. El punto amarillo indica que la aplicación se ha creado y modificado, y que la última configuración modificada aún no se ha publicado.

Proximidad estática

La aplicación Static Proximity responde a la plataforma que se encuentra cerca de la latitud y longitud del usuario solicitante.

> **Nota:**
>
> Todas las aplicaciones de Openmix requieren la configuración previa de un conjunto de plataformas asociadas. Si no encuentra una plataforma en la lista, puede configurarla en la página Plataformas del portal.

Navegación

1. Inicie sesión en el portal NetScaler Intelligent Traffic Management.
2. En el menú de navegación de la izquierda, vaya a **Openmix > Configuración de la aplicación**.
3. Haga clic en el botón con el signo más, **Agregar aplicación Openmix** en la parte superior derecha.
4. Selecciona **Aplicación de inicio rápido**.

Información básica

1. En el cuadro de diálogo **Información básica**, seleccione **DNS** como protocolo.
2. Seleccione **Proximidad estática** como tipo de aplicación. Asigne a la aplicación un nombre (campo obligatorio), una descripción (campo opcional) y una etiqueta (campo opcional).
3. Haga clic en **Siguiente** para configurar.

Configuración

1. Si se activa, el **umbral de disponibilidad** tiene un valor predeterminado del 80%. Introduzca un valor nuevo para reemplazar el valor predeterminado.
2. Introduzca un CNAME/A/AAAA o una dirección IP para **Fallback**. Normalmente, el CNAME/A/AAAA o IP de reserva se utiliza si la aplicación encuentra problemas o errores. Este campo no puede estar vacío.
3. Introduzca **TTL (tiempo de vida)** para la respuesta. El valor predeterminado es de 20 segundos, pero este valor se puede anular si es necesario.
4. Haga clic en **Siguiente** para ver Controles de persistencia.

Controles de persistencia Configure la **persistencia local**. Para obtener más información, consulte Persistencia local. Haga clic en **Siguiente** para obtener información sobre la plataforma.

Información de la plataforma Cada plataforma debe tener su latitud y longitud configuradas a través de la página **Plataformas** . Los alias de las plataformas comunitarias inicialmente heredan la información geográfica de la plataforma comunitaria, aunque después de crear un alias puede cambiarlos. Las plataformas privadas deben configurarse al crearlas o después a través de su panel de

configuración. Para ver el panel de configuración, simplemente haga clic en la entrada Plataforma de la tabla.

Solo las plataformas que pertenecen a las siguientes categorías pueden tener información geográfica y formar parte de la lista de respuestas de una aplicación opx:

- Computación en nube
- Almacenamiento en la nube
- Centro de datos

1. Seleccione una plataforma de la lista **Plataforma**.
2. Introduzca un registro CNAME o A/AAAA o IP (en DNS) o URL (en HTTP) para la plataforma. Debe ser una dirección URL, un nombre de host o una dirección IP válidos. Puede tener la forma de:

   ```
   scheme:[//host[:port]][/path][?query][#fragment]
   ```

3. Asegúrese de que la casilla de verificación **Activado** esté activada para indicar que la plataforma está habilitada antes de pasar al siguiente paso.
4. Si Sonar está disponible para esta plataforma y desea utilizar los datos de Sonar para que se tengan en cuenta durante la resolución de DNS, asegúrese de hacer clic en la casilla de verificación **Usar Sonar para la disponibilidad de la plataforma** .
5. Puede agregar más plataformas haciendo clic en **Agregar plataforma**.
6. Haga clic en **Siguiente** para **Configuración de ubicación**.

Configuración de ubicación

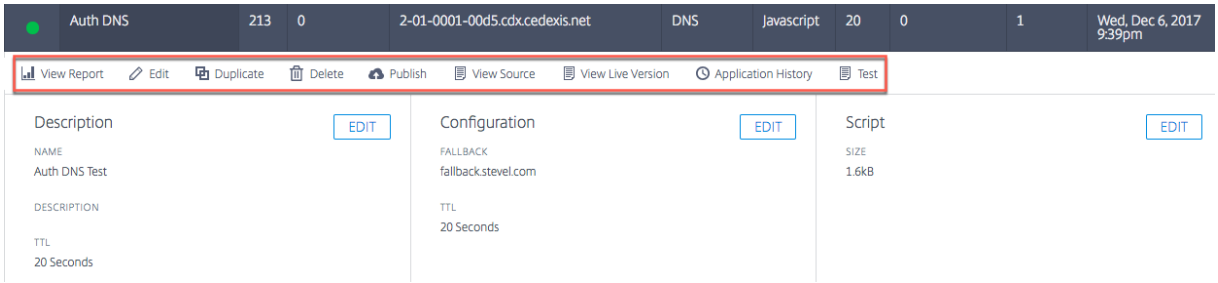
1. En la parte Global del cuadro de diálogo Configuración de ubicación, puede configurar una cadena de plataformas para el enrutamiento global. Puede activar o desactivar la selección de cada plataforma de forma global.
2. En Mercados y países, puede crear diferentes configuraciones por mercado o país, teniendo efectivamente reglas de geocercas para ellas.
3. Haga clic en **Completar** para crear la solicitud.

En la ventana emergente de confirmación, haz clic en **Publicar, Agregar otro** o **Listo**:

- Si haces clic en **Publicar**, la aplicación se activa al instante y el estado es verde. Esto significa que la aplicación está en producción.
- Si **hace clic en Listo**, la aplicación aparece en la página de Openmix, pero no se ha publicado y el estado es rojo.
- Si hace clic en **Agregar otra**, el estado de la aplicación es el mismo que **Listo**, pero reinicia el mismo proceso para crear una nueva aplicación.

Administración de aplicaciones de inicio rápido

Utilice las fichas superiores del panel del administrador de aplicaciones para modificar, duplicar, eliminar, probar, ver informes, ver la fuente y ver el historial de versiones de la aplicación. Haga clic en su aplicación en la página de lista de aplicaciones de Openmix para expandir el administrador de aplicaciones.



Ver informe

Ver informe le lleva a la página Informes de decisión de Openmix, donde puede ver la tendencia de las decisiones de Openmix para cada una de sus aplicaciones, plataformas y geografías.

Modificar

Para modificar su aplicación Openmix, simplemente haga clic en el icono **Modificar** en la parte superior del panel del administrador de aplicaciones. También puede realizar ediciones individuales por separado para obtener información básica, configuración, plataforma o ubicación haciendo clic en los botones **Modificar** del panel, como se muestra en la figura. Cuando termine de modificar, haga clic en **Listo**para mostrar la aplicación con un estado sin publicar (para más ediciones más adelante) o haga clic en **Publicar**para entrar en directo al instante.

Duplicado

Haga clic en **Duplicar** para replicar la configuración de la aplicación actual y guardarla con un nombre nuevo.

Eliminar

Haga clic en **Eliminar**para quitar aplicaciones que ya no necesite.

Publicar

Haga clic en **Publicar** para publicar directamente la aplicación desde el administrador de aplicaciones de Openmix. Esta opción solo es visible si la aplicación aún no se ha publicado.

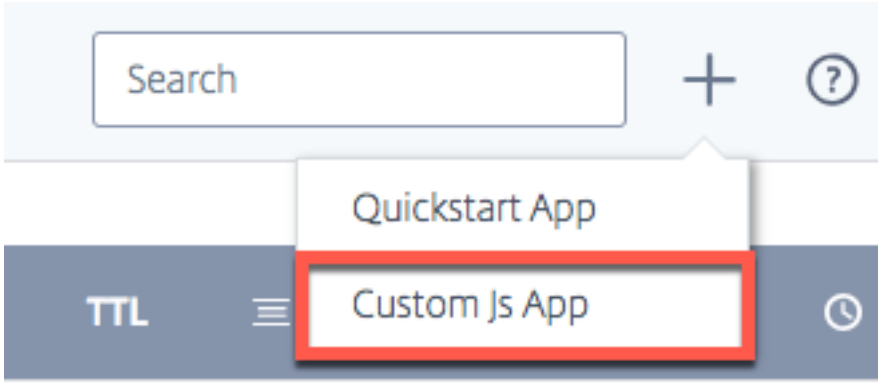
Aplicaciones JavaScript personalizadas de Openmix

Las aplicaciones JavaScript de Openmix son aplicaciones con scripts Java personalizables. Puede crear, configurar, probar y publicar mediante la interfaz de usuario del portal de ITM.

Nota: Esta guía no cubre la creación real del script personalizado (sintaxis, variables, etc.). Para obtener más información sobre la creación de JavaScript personalizado, consulte Developer Exchange.

Navegación

1. Inicie sesión en el portal ITM.
2. Desde el menú de navegación de la izquierda, vaya a **Openmix**.
3. Elija **Configuración de la aplicación**.
4. Para configurar una nueva aplicación Openmix, haz clic en el icono de agregar en la esquina superior derecha.
5. Seleccione **Aplicación JS personalizada**.
6. Se abrirá la página **Configuración de la aplicación Openmix**.



Información básica

1. **Nombre de la aplicación**: asigne un nombre a su aplicación.
2. **Descripción**: Dar a la aplicación una descripción o agregar una nota de lanzamiento aquí. Es un campo opcional.

3. **Etiquetas**: Introduzca una etiqueta adecuada, si es necesario. Las etiquetas ayudan a identificar y organizar la aplicación. Es un campo opcional.
4. **Protocolo**: seleccione DNS o HTTP como protocolo.
   - **DNS**: si selecciona DNS, se debe introducir un valor TTL.
   - **HTTP**: Si selecciona HTTP, puede habilitar **Secure Access**.
5. **TTL**: Introduzca un tiempo de vida DNS para la aplicación. El valor recomendado es de 20 segundos. Nota: Este TTL se aplica si no hay TTL establecido por la aplicación JS personalizada o si la respuesta es un valor de reserva.
6. **Fallback**: Introduzca una dirección CNAME/A/AAAA o IP para **Fallback**. Normalmente, el CNAME/A/AAAA o IP de reserva se utiliza si la aplicación encuentra problemas o errores.
7. **Acceso seguro**: si **Secure Access**está habilitado, la API HTTP debe requerir una clave de acceso Oauth del cliente cuando se llama. Consulte Protección de la API HTTP de Openmix para obtener más información.

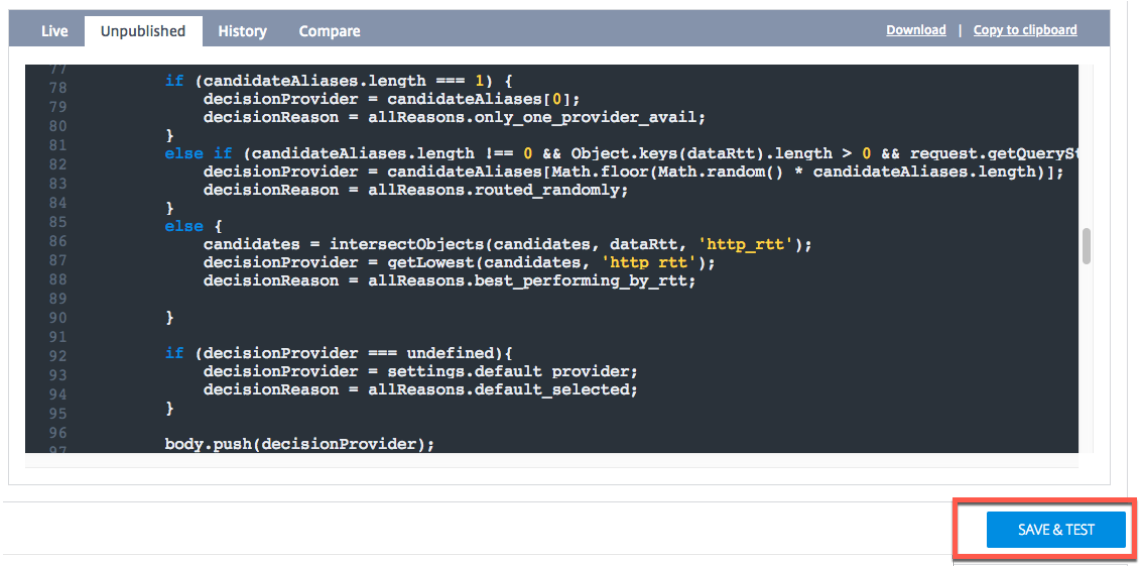
   Nota: Al habilitar el acceso seguro, se muestra un icono de candado junto al nombre de la aplicación en la lista de aplicaciones en la página principal de Openmix.

JavaScript personalizado

Una vez que introduzca la información de configuración, puede cargar su JavaScript personalizado.

1. Haga clic en el botón **Elegir archivo** y seleccione el archivo JavaScript que quiere cargar. Puede cargar un archivo nuevo para sobrescribir uno existente en cualquier momento.
2. Haga clic en **Guardar y probar** para guardar la aplicación.

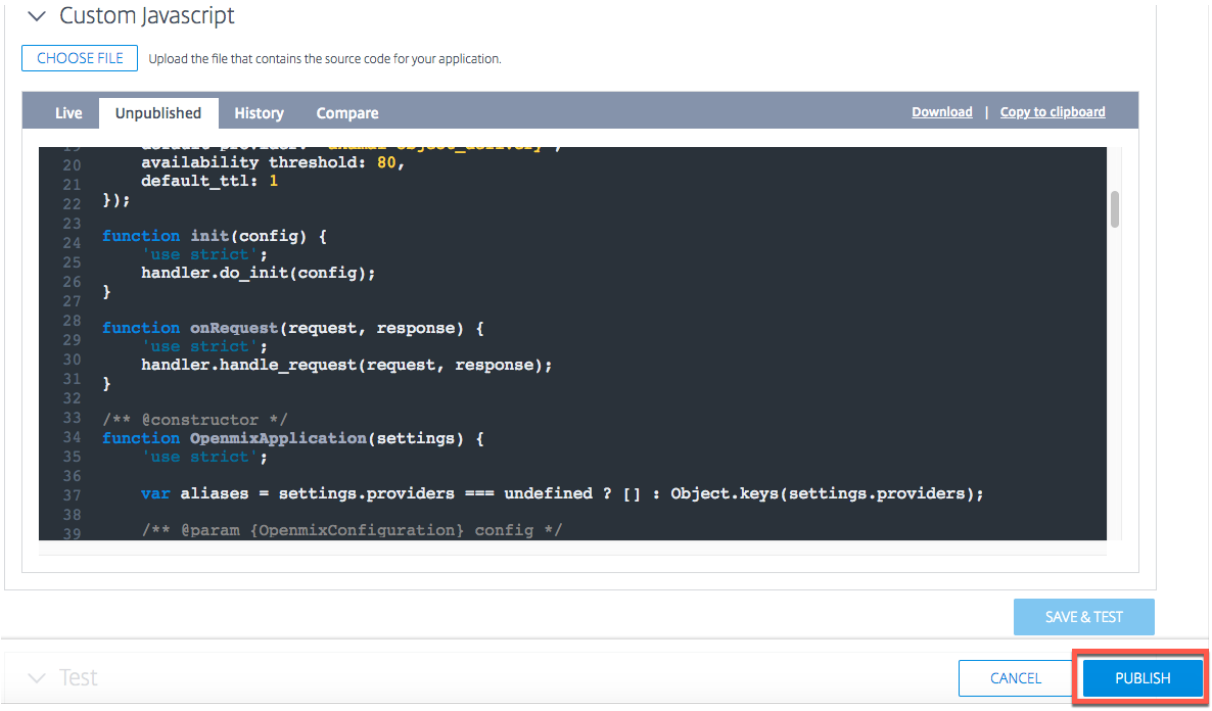
   Nota: La aplicación se prueba automáticamente con un comprobador de aplicaciones cuando se carga y se guarda. Si hay errores, el verificador de la aplicación muestra la información del error y la ubicación del error. Para obtener más información sobre los datos disponibles en el comprobador de aplicaciones, consulte la sección Verificación de aplicaciones .



3. Haga clic en **Cancelar** para volver a la página Aplicaciones Openmix o haga clic en **Publicar** si está listo para que la aplicación entre en marcha.

   Nota: Si hace clic en **Publicar**, la aplicación se activa al instante y tiene un estado verde. Su aplicación está en producción.

   Si hace clic en **Cancelar**, la aplicación aparece en la página de aplicaciones, pero no se ha publicado y el estado es rojo. Para obtener más información sobre el estado, consulte la sección Estado de la solicitud.



Implementación de aplicaciones por etapas

Puedes gestionar la implementación de tu aplicación enviando un pequeño porcentaje de tu tráfico web a través de una nueva versión, a veces llamada Canary Deployment. ITM le permite enviar un porcentaje específico de tráfico a la nueva versión de una aplicación para garantizar que la lógica de la aplicación se comporte como se espera. Puede informar sobre el comportamiento de las versiones existentes y nuevas para evaluar los cambios realizados en su aplicación en un entorno activo. Esta opción le permite corregir cualquier problema o anomalía que se produzca antes de dirigir el 100% de su tráfico web a través de la aplicación recién modificada. Después de verificar el comportamiento deseado, puede aumentar el porcentaje de tráfico a la versión más reciente o implementar la aplicación para todos los usuarios.

Para organizar la implementación de la aplicación y lanzar una versión de prueba de la aplicación recién modificada, haga lo siguiente:

- Haga clic en el nombre de la aplicación (en la página de lista de aplicaciones Openmix). Se abrirá el panel del administrador de aplicaciones.
- Haga clic en el icono **Modificar** para modificar tu aplicación.
- Modifique su aplicación existente con todos los cambios necesarios.
- Una vez que haya terminado con los cambios, haga clic en **Guardar y probar**.
- Desplázate hacia abajo en la parte inferior de la página con los botones **Cancelar** y **Publicar** . Introduzca el porcentaje de tráfico web (del 1% al 99%) que desea que fluya a través de esta versión recientemente modificada.
- Marque la casilla de distribución parcial del tráfico a través de esta nueva versión de la aplicación. El tráfico restante se envía a la versión en vivo anterior.
- Haga clic en **Publicar**. Esta nueva versión de prueba de la aplicación ahora aparece en la lista de aplicaciones de la página **Configuración de Openmix** con un nuevo icono de **estado** . El nuevo icono **Estado** indica que solo el tráfico web parcial fluye en vivo a través de esta versión.

Puede modificar el flujo de tráfico a la versión de prueba y cambiar el porcentaje del flujo de tráfico para ver el rendimiento.

```
1 ![Canary](/en-us/citrix-intelligent-traffic-management/media/openmix-
    jsapp-edit-canary.png)
```

Para comprobar el rendimiento de su aplicación, vaya al Informe de decisión de Openmix. Seleccione **Aplicación** como dimensión principal y **Versión** como dimensión secundaria. A continuación, haga clic en **Aplicar filtros** después de seleccionar la aplicación de la lista. El gráfico muestra el rendimiento de las diferentes versiones de la aplicación.

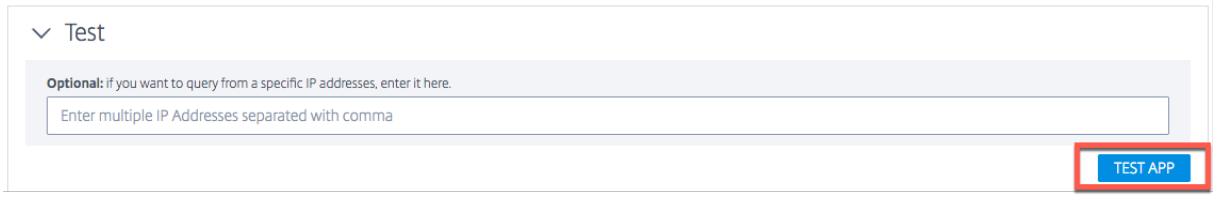
Una vez que esté satisfecho con el rendimiento de esta versión de la aplicación, puede continuar y dirigir el 100% de su tráfico web a través de ella haciendo clic en el **botón** Publicar.

Esta versión reemplaza la versión actual por la versión recién modificada.

Si no quiere activar esta versión, haga clic en **Anular publicación**. Los cambios se guardan y aparecen como una aplicación no publicada en la lista de aplicaciones de la página **Configuración de Openmix**. Ahora el 100% de su tráfico web fluye a través de la versión actual en vivo de su aplicación.

Prueba

Puede probar su aplicación JavaScript utilizando el botón **Probar aplicación** antes o después de la publicación.

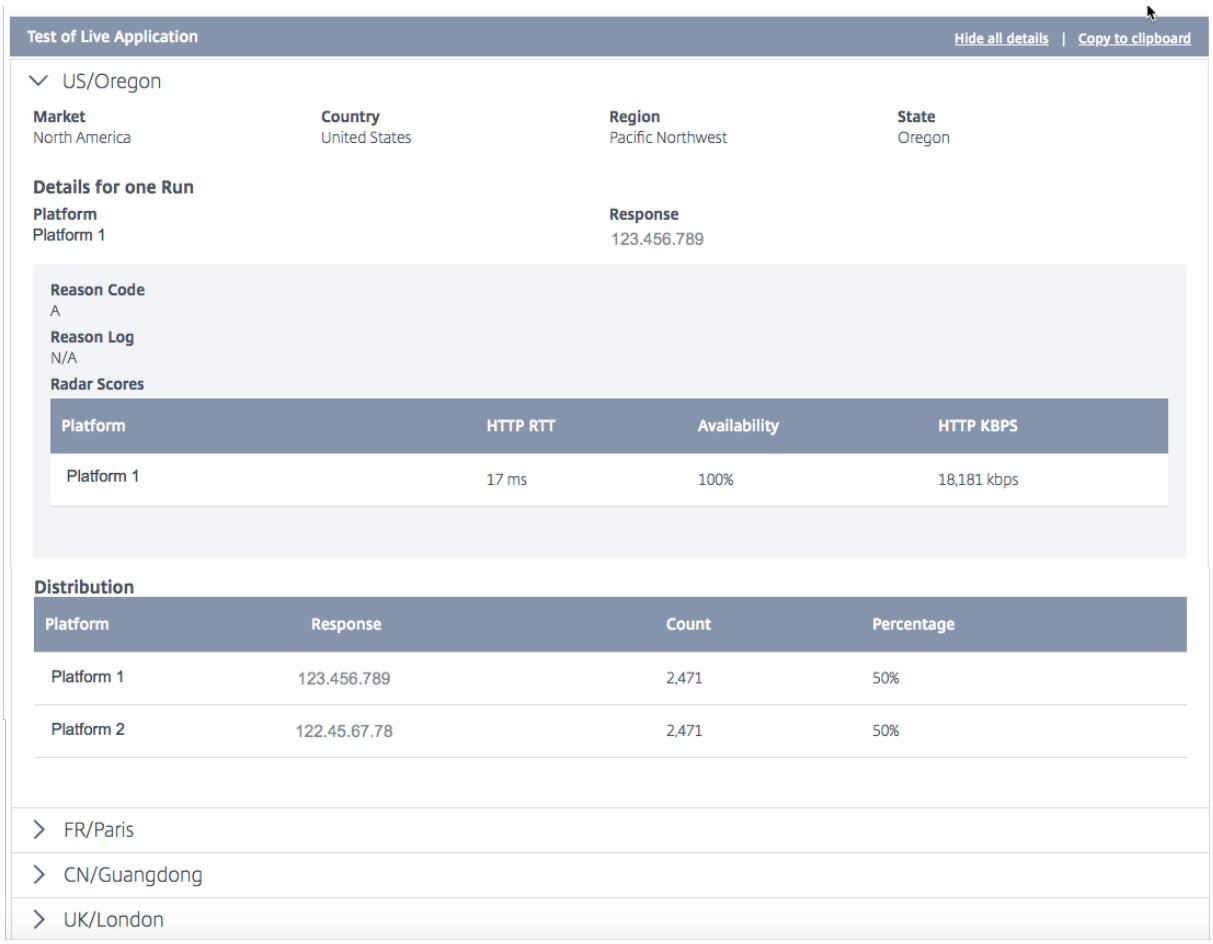


Le permite ver los resultados de las pruebas en conjuntos específicos de mercados, países, regiones y estados. Puedes consultar la aplicación desde direcciones IP específicas.

Los resultados de las pruebas incluyen, **Plataforma** seleccionada por la aplicación, **Respuesta** recibida, **Código** de **razón, Registro** de razón, **Resultados de Radar**, **Distribución**, etc.

Esta función también le permite ver la distribución de decisiones en diferentes plataformas. Por ejemplo, si se utilizan dos plataformas para el enrutamiento, puede ver el número de decisiones y la respuesta recibida para cada una de ellas.

Haga clic en el enlace **Mostrar todos los detalles** para ver los resultados de las pruebas de tu aplicación.



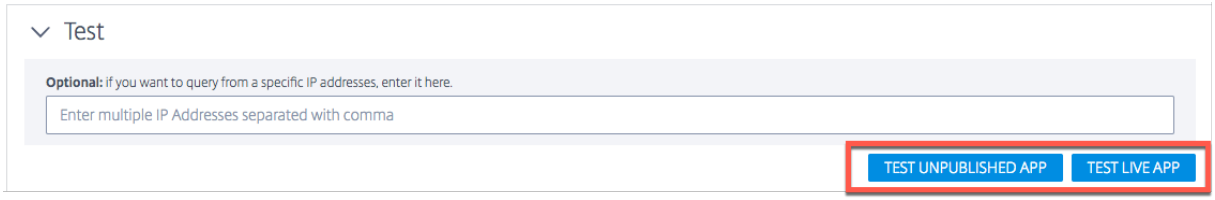
Los siguientes valores se muestran como resultados de la prueba:

Campo	Descripción
Mercado, País, Región y Estado	La ubicación en la que se probó la aplicación.
Plataforma	La plataforma seleccionada por la aplicación.
Respuesta	El CNAME o la dirección IP de la plataforma seleccionada por la aplicación.
Código de motivo	Describe el motivo detrás de la decisión.
Registro de motivos	Salida de la aplicación definida por el cliente. Permite a los clientes registrar información sobre las decisiones sobre las aplicaciones.
Puntuación de Radar	Las mediciones de **tiempo de respuesta (RTT)**, **disponibilidad**y **rendimiento**registradas para la plataforma.

Campo	Descripción
Distribución	La distribución de plataformas que selecciona una aplicación para cada ubicación que se prueba. El **recuento** representa el número de veces que se seleccionó la plataforma. Y el **Porcentaje** es el porcentaje del recuento total para la selección de la plataforma.

Nota: Puede ejecutar esta prueba en la aplicación en vivo o en la versión no publicada, es decir, si la aplicación aún no está publicada.

Una vez publicada la aplicación, tiene la opción de probar la aplicación en vivo haciendo clic en la opción **Probar aplicación en vivo**. Si modifica la aplicación o carga una nueva versión, puede probarla antes de publicarla haciendo clic en el botón **Probar aplicación no publicada**.



Verificación de la aplicación

Para garantizar que las aplicaciones JavaScript personalizadas se comporten como se espera, ejecute la aplicación a través de un verificador de código y lógica cuando la cargue en el Portal de ITM. El verificador de aplicaciones ejecuta la aplicación a través de un servidor de decisiones con tráfico sintético para comprobar si la aplicación se compila y se ejecuta correctamente.

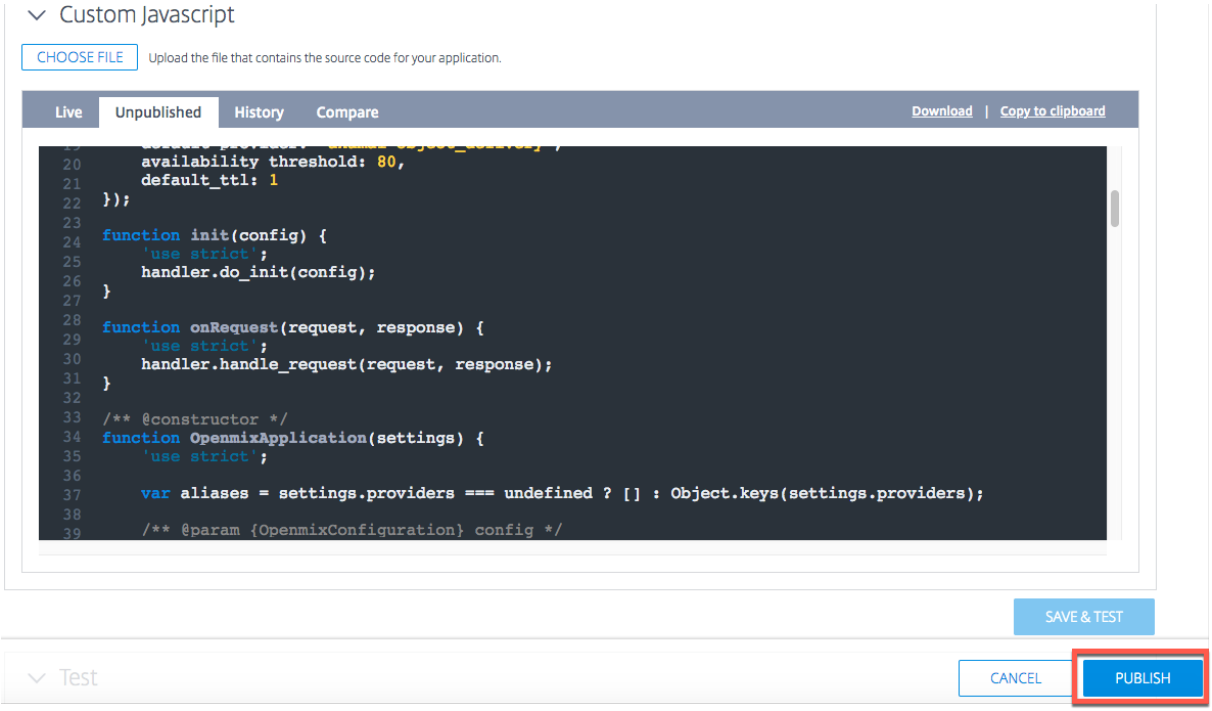
Si la aplicación se ejecuta sin errores, el verificador proporciona información sobre la distribución de la decisión y las características de ejecución. Por otro lado, si el servidor de decisiones encuentra un error mientras ejecuta la aplicación, el verificador proporciona información sobre el error. Recomendamos que la aplicación no contenga errores antes de publicarla.

En caso de errores, puede corregir el archivo JavaScript en su local y volver a subirlo al Portal haciendo clic en el botón **Elegir archivo**.

Publicar

Para publicar tu aplicación y que se publique, haz clic en el botón **Publicar**. Esta opción aparece atenuada si la aplicación aún no está guardada o ya publicada. Cuando la aplicación se activa, aparece

en la página del administrador de aplicaciones de Openmix con un estado verde. Para obtener más información sobre el estado de la aplicación, consulte la sección Estado de la aplicación.

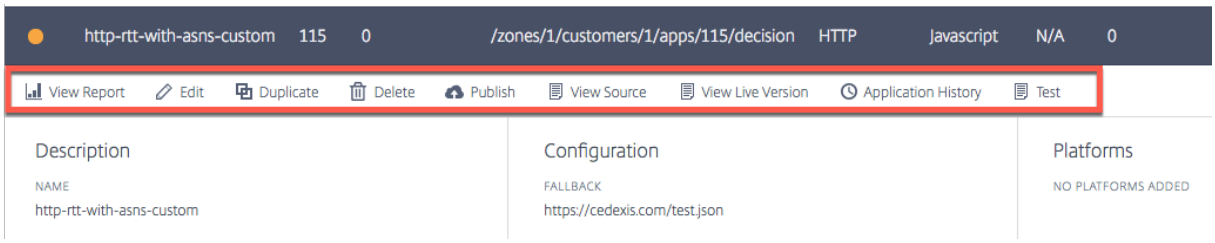


Nota: La aplicación se publica con errores si es necesario.

Administración de aplicaciones JavaScript personalizadas

Utilice las fichas superiores del panel del administrador de aplicaciones para ver informes, modificar, duplicar, eliminar, publicar, ver el código fuente, ver la versión en vivo y ver el historial.

Haga clic en su aplicación en la página de lista de aplicaciones de Openmix para expandir el panel del administrador de aplicaciones.

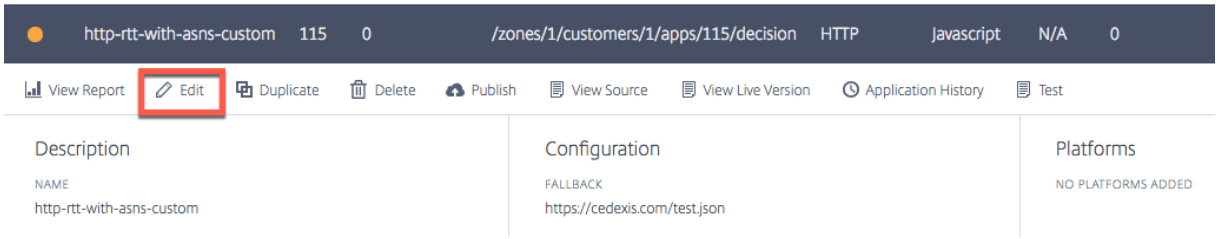


Ver informe

Ver informe le lleva a la página **Informes de decisión de Openmix**, donde puede ver la tendencia de las decisiones de Openmix para cada una de sus aplicaciones, plataformas y geografías.

Modificar

Para modificar una aplicación JavaScript personalizada de Openmix, haga clic en el nombre de la aplicación (en la página de lista de aplicaciones Openmix). Se abrirá el panel del administrador de aplicaciones. Se pueden realizar cambios y actualizaciones en la configuración haciendo clic en el icono **Modificar**.



Ver origen

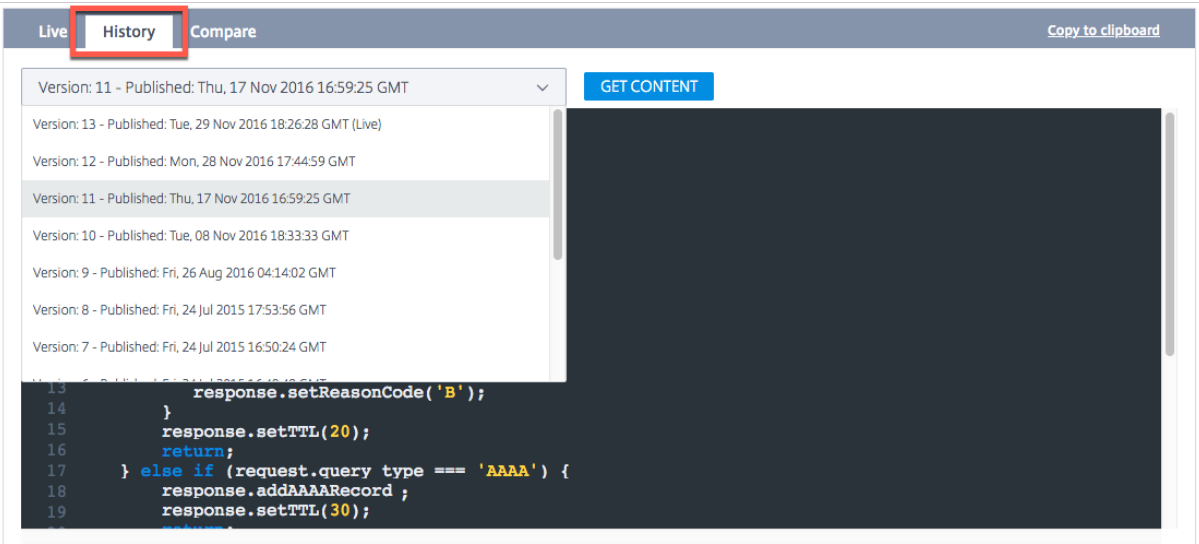
View Source le permite ver la fuente JavaScript de la aplicación, es decir, la última versión de la aplicación, ya sea que se haya publicado. Esta opción solo está disponible para aplicaciones JavaScript personalizadas.

Ver versión en vivo

Puedes ver, copiar y descargar la última versión publicada de la aplicación. Esta opción solo está disponible para aplicaciones JavaScript personalizadas.

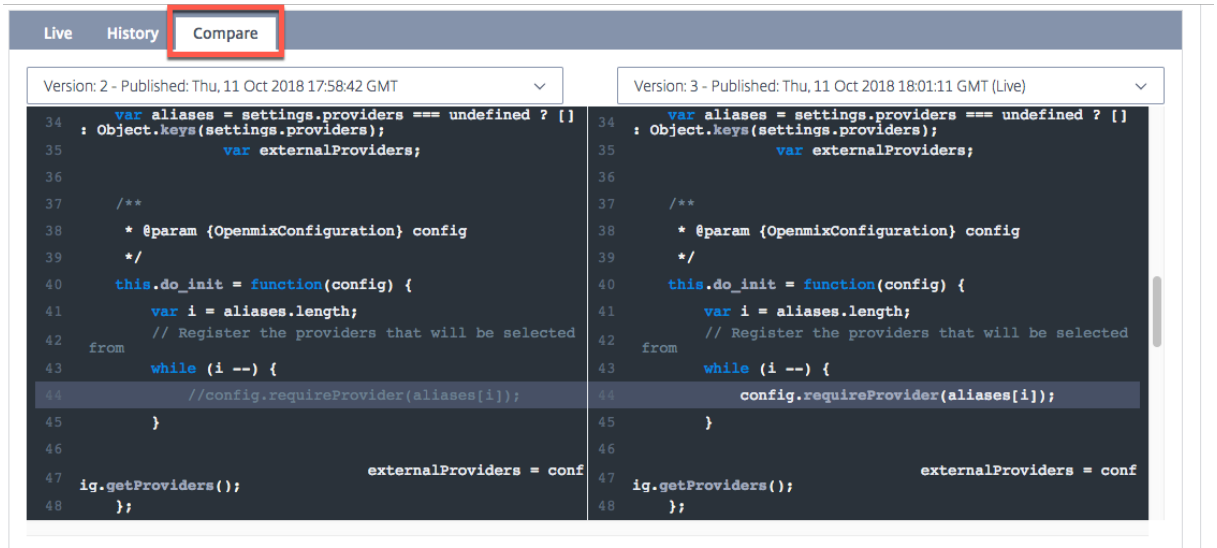
Historial de aplicaciones

Historial de aplicaciones le permite ver diferentes versiones de la aplicación. Puede utilizar la lista **Seleccionar una versión** para cambiar de una versión activa a una versión anterior. Haga clic en **Obtener contenido** para cambiar a la versión anterior. Esta opción solo está disponible para aplicaciones JavaScript personalizadas.



Comparar

La función **Comparar** le permite comparar diferentes versiones de su archivo JavaScript. Puedes ver claramente las diferencias entre las dos versiones de tu app con líneas de guion resaltadas.



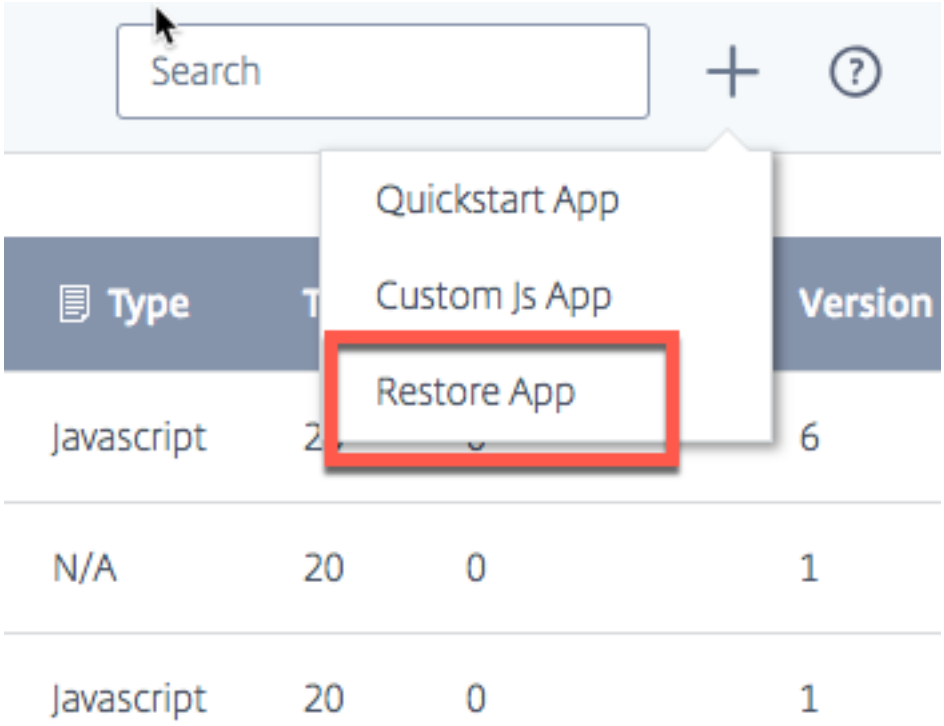
Eliminar

Para eliminar una aplicación Openmix, haga clic en el nombre de la aplicación (en la página de lista de aplicaciones Openmix). Se abrirá el panel del administrador de aplicaciones. Haga clic en el icono **Eliminar** y, a continuación, elija el botón **Eliminar** en el cuadro de diálogo de confirmación. La aplicación desaparece de la lista.

Restaurar aplicación

La función **Restaurar aplicación** le permite volver a habilitar una aplicación después de que se haya eliminado.
Para restaurar una aplicación, haga lo siguiente:

1. Haga clic en el icono **Agregar +** en la parte superior derecha de la página.
2. Selecciona **Restaurar aplicación** en el menú implementable. Se abrirá **la ventana Restaurar aplicación**.



3. Busque la aplicación que quiere volver a habilitar en la lista y haga clic en el botón **Restaurar** correspondiente.

La aplicación vuelve a aparecer en la lista de la página de Openmix con el mismo estado.

Persistencia local

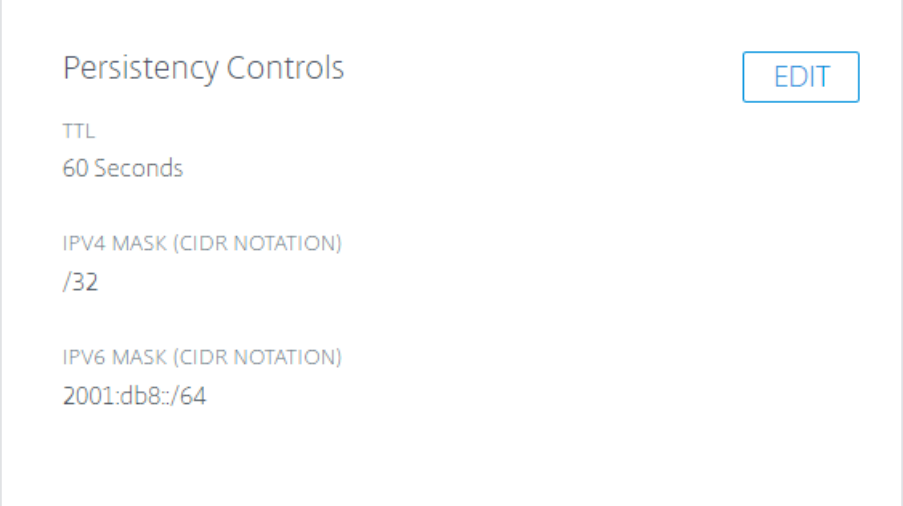
La función de **persistencia local** ofrece la capacidad de mantener la firmeza de las decisiones cuando está habilitada para una aplicación Openmix. Las solicitudes se identifican mediante la máscara de subred IP, cuya longitud se puede configurar. Por ejemplo, cuando un cliente repite una solicitud a la misma aplicación dentro de un período determinado, se devuelve la decisión original. Puede ser una función esencial cuando se requiere que un cliente no se balancee entre diferentes decisiones durante una sesión en particular. Está disponible para aplicaciones Openmix DNS o HTTP.

Debido a las restricciones naturales subyacentes del mecanismo, no se garantiza la persistencia del 100% de las solicitudes. En cambio, se aplica un enfoque de mejor esfuerzo. Las pruebas han demostrado que la precisión de persistencia esperada está en el rango del 95 al 97%.

> **Nota:**
>
> Para habilitar la función de persistencia local en su cuenta, cree un tíquet de asistencia o contacte con su administrador de satisfacción de clientes. Además, se requiere una zona DNS predictiva, configurada con servidores de nombres `ns5.cedexis.net` y `ns6.cedexis.net`. Tenga en cuenta la cantidad significativa de tiempo que las actualizaciones de la zona DNS pueden requerir para propagarse a través de Internet.

Configuración

Para habilitar la persistencia local, seleccione **Controles de persistencia > Modificar**, en las opciones de la aplicación Openmix.



Los ajustes disponibles son los siguientes:

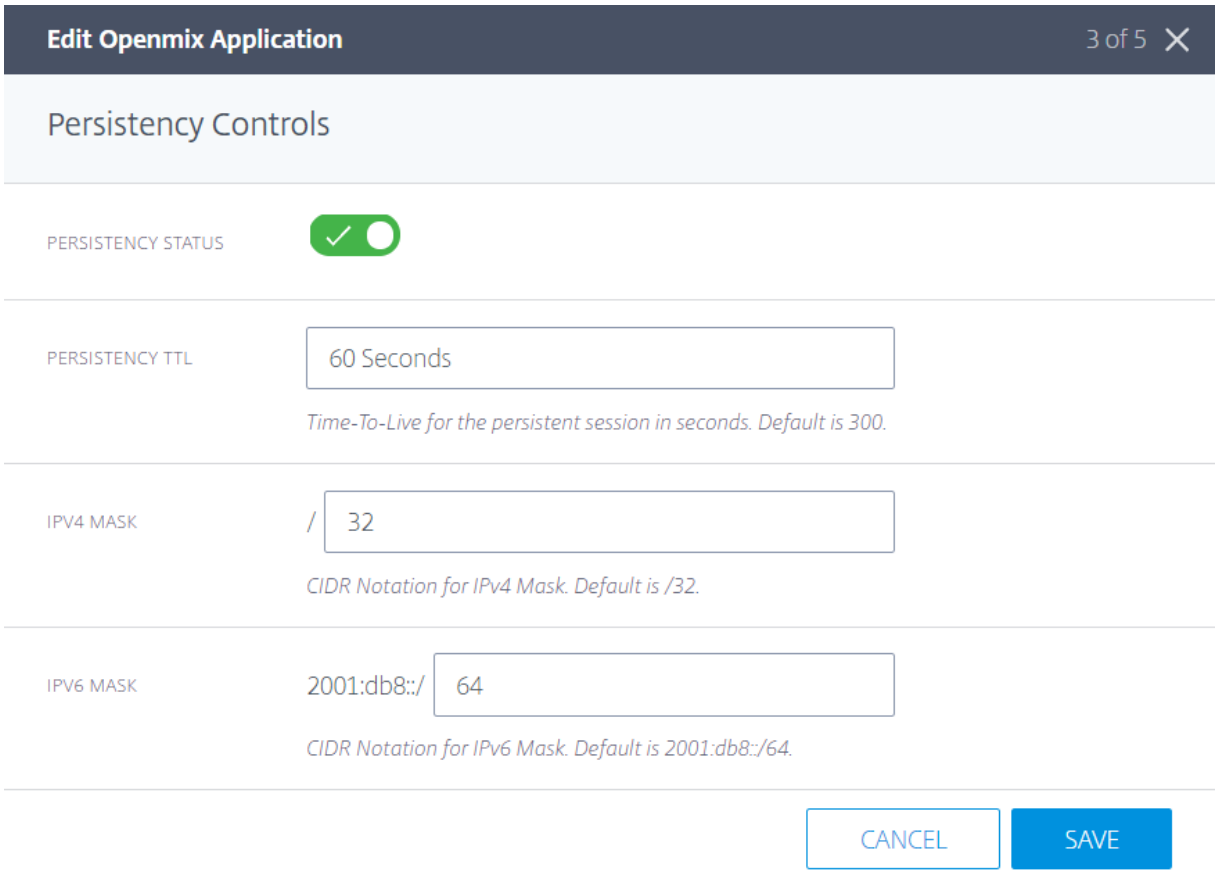
1. En el cuadro de diálogo Configuración, introduzca el **TTL de persistencia**. La opción predeterminada es de 300 segundos. Se permiten valores entre 60 y 1440. Después de una solicitud

inicial, la decisión de DNS servida se mantiene durante un máximo de 300 segundos. Si otra solicitud proviene del mismo rango de subredes IP del sistema antes del vencimiento, se toma la misma decisión.

2. Se proporcionan máscaras IPv4 e IPv6 para establecer la granularidad de la persistencia persistente. El valor predeterminado es "/32"y "/64", para IPv4 e IPv6, respectivamente. Los valores permitidos son:

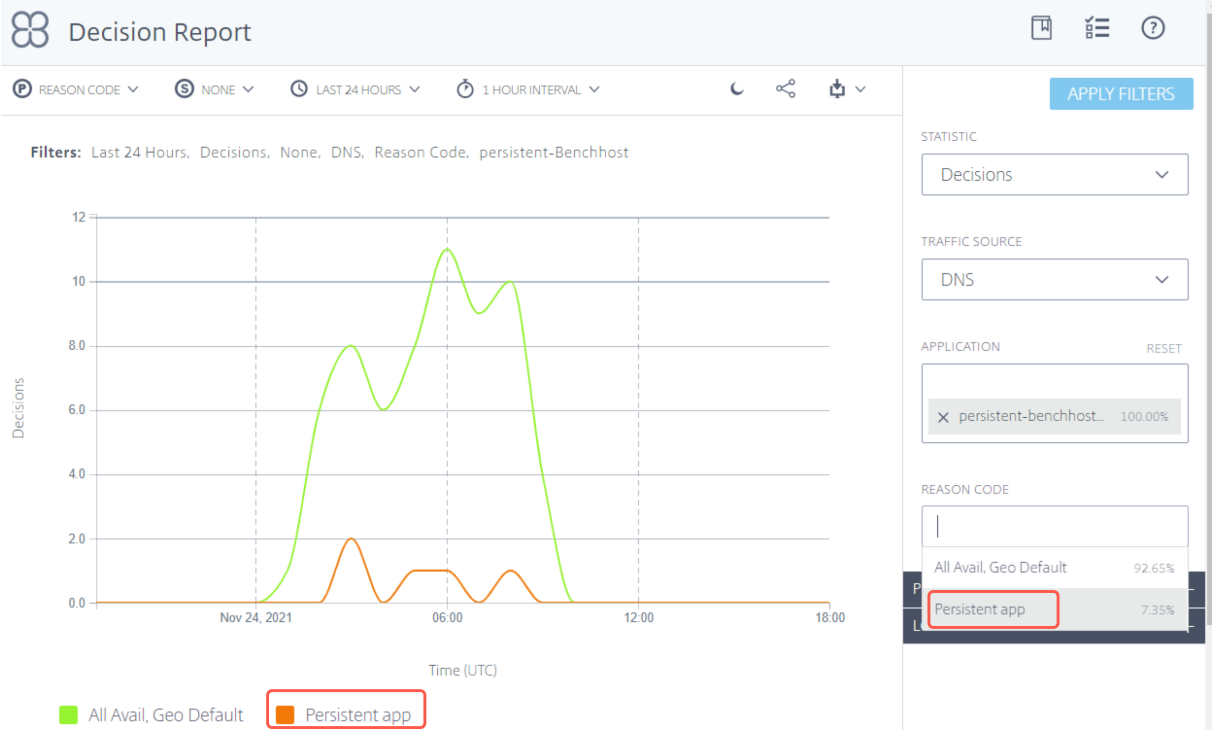
   - /8 hasta /32, para IPv4
   - /32 hasta /64, para IPv6

   Este enmascaramiento en la dirección IP del cliente determina la clave de persistencia utilizada en el almacén de datos interno. Por ejemplo, si dos (o más) IP de cliente se asignan a la misma dirección IP enmascarada, se les sirve con la misma decisión persistente.



La misma configuración también está disponible en la configuración de la aplicación predictiva.

Las decisiones de Openmix que se proporcionan a través del almacén de datos interno se informan con el código de motivo de la **aplicación Persistente** en el Informe de decisiones.



Comprobaciones de estado

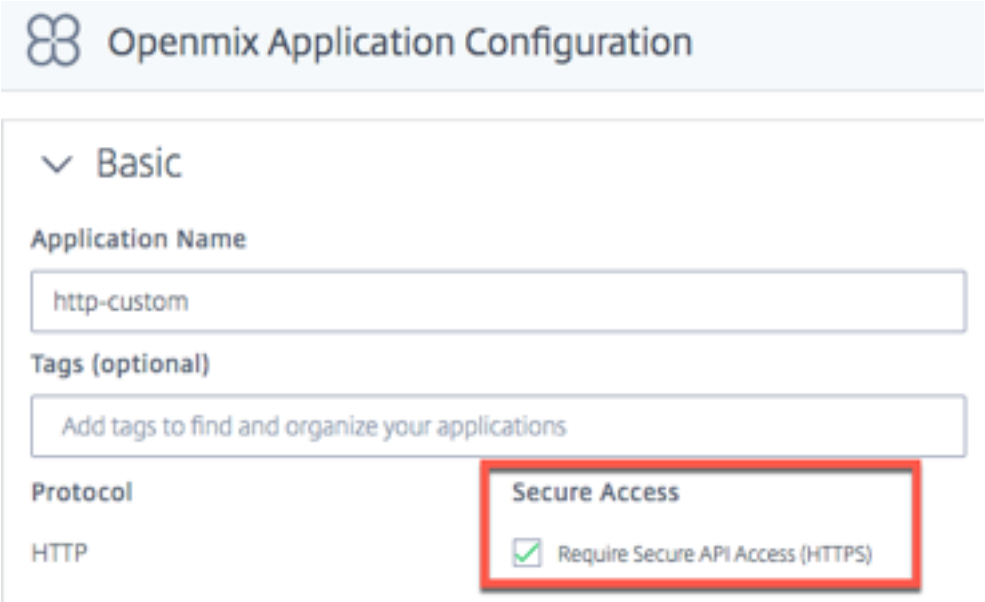
Las decisiones que se sirven desde la memoria caché de persistencia están sujetas a comprobaciones de estado adicionales antes de que se entreguen:

1. Si la aplicación está configurada con **Sonar Availability Check**, se comprueba el estado de disponibilidad de Sonar antes de que se sirva una decisión almacenada en caché. Si Sonar informa que la plataforma está “inactiva”, la decisión de almacenamiento en caché se ignora y la aplicación OpenMix se ejecuta de nuevo.
2. Si la aplicación está configurada con **Radar Availability Check**, se comprueba el estado de disponibilidad de Radar antes de que se sirva una decisión almacenada en caché. Si la disponibilidad de la plataforma es inferior al umbral configurado, se ignora la decisión de almacenamiento en caché.

> **Nota:**
>
> Para la persistencia, el umbral máximo para el estado de disponibilidad de Radar se establece en un 10% fijo.

Protección de la API HTTP de Openmix

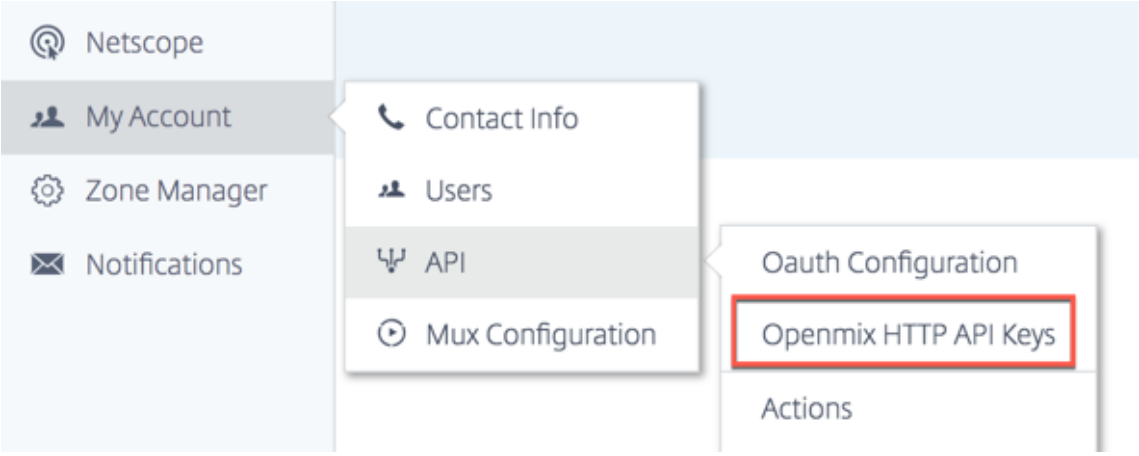
Openmix está disponible a través de DNS o una API HTTP para la integración en flujos de trabajo que no sean DNS. De forma predeterminada, la API HTTP se llama a través de HTTP simple. La API también se puede proteger a través de TLS y autenticación de clave. Se hace a través de la interfaz de usuario marcando la casilla **Requerir acceso seguro a la API (HTTPS)**.



Creación de claves API

Para habilitar la autenticación de claves, haga lo siguiente.

1. Seleccione la casilla **Requerir acceso seguro a la API (HTTPS)** en la página **Configuración de aplicaciones de Openmix** para activar el acceso seguro para cada aplicación.
2. Para generar una clave de acceso segura, vaya a **Mi cuenta** -> **API** -> **Openmix HTTP API Keys**



3. Si eres usuario por primera vez, se te pedirá que comiences introduciendo tu ID de cliente. Introduzca su **ID de cliente** en el cuadro de diálogo **Nuevo cliente** y haga clic en **Completar**.
4. La clave **secreta de cliente** se muestra junto al **ID de cliente** en la página **Configuración de autenticación de API HTTP de Openmix**.
5. Ahora puede hacer una solicitud a la aplicación Openmix utilizando la autenticación básica. Utilice su **ID de cliente** como nombre de usuario y el **secreto de cliente** como contraseña para invocar la aplicación en el explorador.

   Para invocar la aplicación mediante la línea de comandos, usa el siguiente comando cURL:

```
curl https://hopx.cedexis.com/zones/<zone>/customers/<customer_id
   >/apps/<app_id>/decision --user <client_key>:<client_secret>
<!--NeedCopy-->
```

Nota: Las claves que cree le dan acceso a cualquiera de sus aplicaciones Openmix.

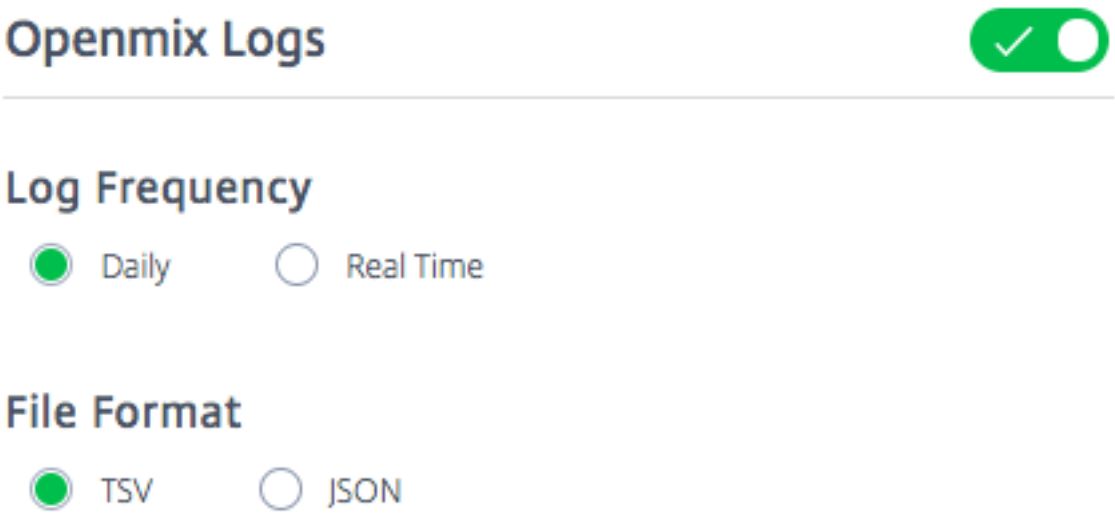
Para obtener más información sobre cómo llamar a la API HTTP de Openmix, consulte la documentación de uso de la API HTTP de Openmix.

Eliminación de claves de API

1. Para eliminar una clave, vaya a la página **Configuración de autenticación de API HTTP de Openmix**.
2. Haga clic en el **ID de cliente**.
3. Seleccione **Eliminar** en la lista. La llave se retira del sistema. No es válido para la autenticación o el acceso seguro a la aplicación Openmix.

Acceso a registros

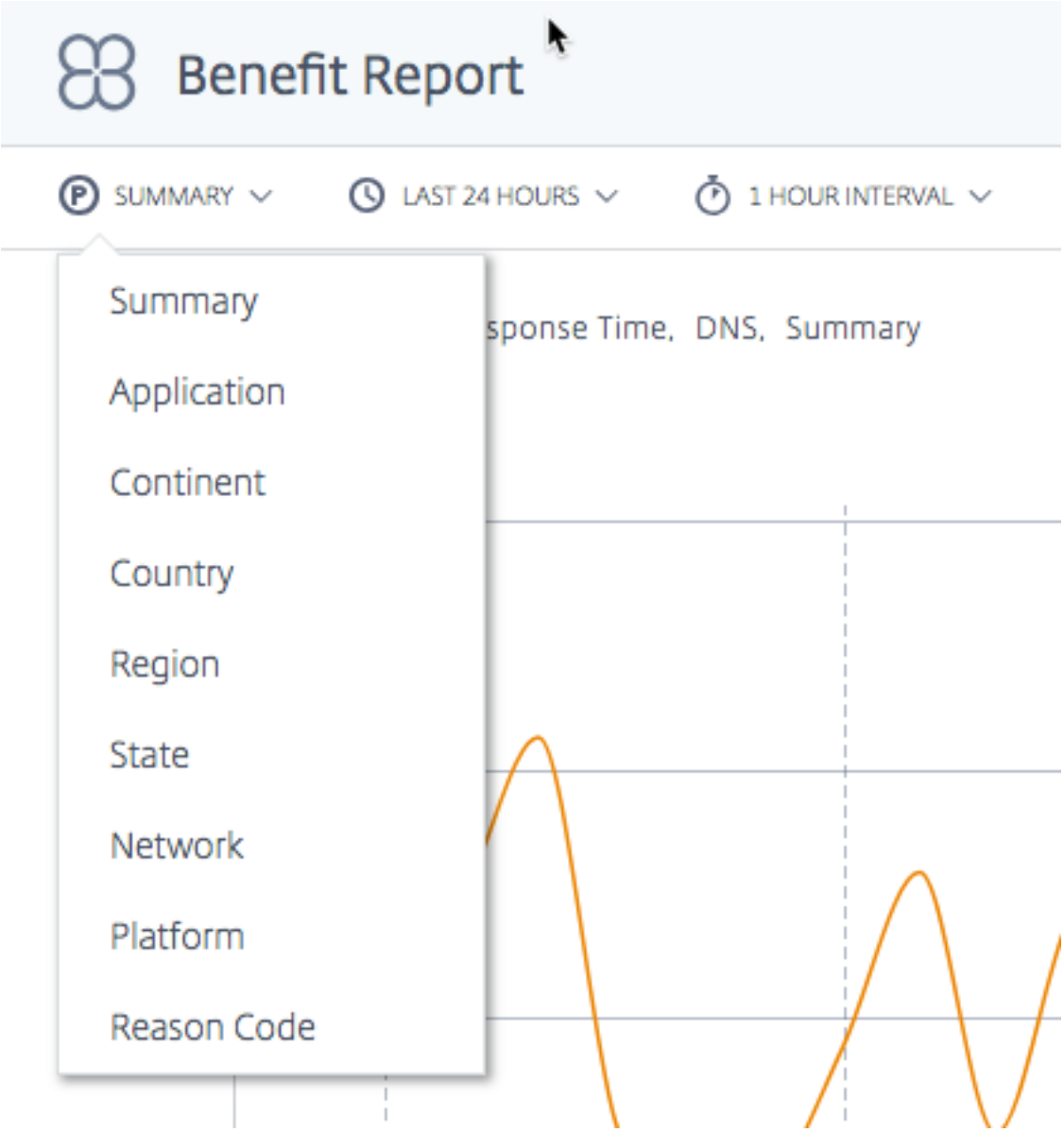
El registro de decisiones tomadas por Openmix se puede recopilar y poner a disposición para su descarga segura. Estos registros pueden ayudarle a analizar las decisiones tomadas por su aplicación Openmix y el comportamiento de la solicitud de depuración. Los registros se pueden activar/desactivar y asegurar a nivel de cuenta. Para obtener más información sobre cómo habilitar y descargar los registros de Openmix y ver las descripciones de los registros, vaya a Netscope.



Informes de Openmix

Los informes de Openmix proporcionan una gran visibilidad de las decisiones de Openmix que se tomaron para el tráfico DNS o HTTP. Cada informe se define en la siguiente sección, pero estos son algunos aspectos importantes de los informes:

Cotas primaria y secundaria

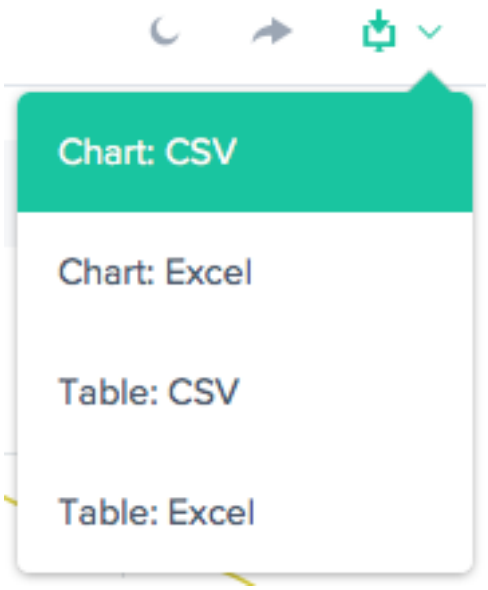


La dimensión principal del gráfico se selecciona a través de una lista por encima del gráfico. Utilice esta lista como un poderoso pivote en el informe. También se puede elegir una dimensión secundaria para refinar aún más los informes.

Alternar fondo de visualización

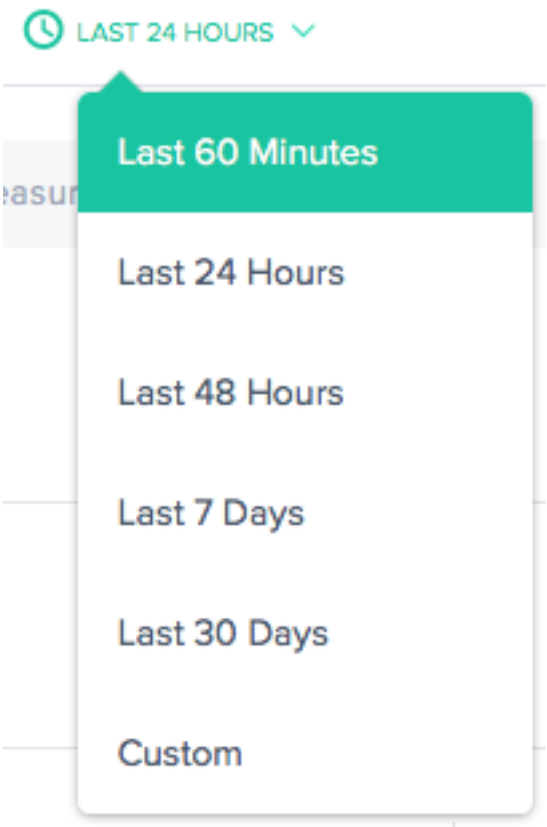
Los gráficos se establecen en un fondo blanco de forma predeterminada. Alternar el fondo a un color oscuro para los monitores de alto contraste mediante la alternancia de fondo.

Exportación de datos



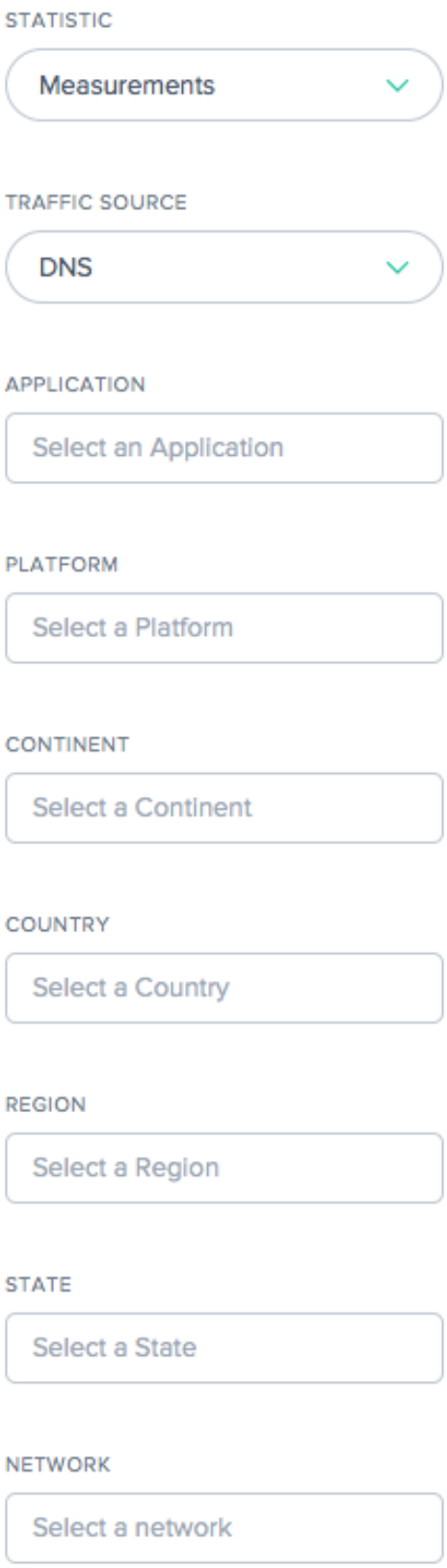
Además, el usuario final puede descargar los datos del gráfico y de la tabla a través del enlace de descarga en la parte superior del informe.

Filtro: Rango de tiempo del informe



Puede generar un informe con un intervalo de tiempo de los últimos 60 minutos, 24 horas, 48 horas, 7 días, 30 días o un intervalo personalizado. La vista predeterminada es las últimas 24 horas.

Filtros: Potentes capacidades de obtención de detalles



Los informes varían ligeramente en términos de qué filtros son apropiados en función de los datos. Los siguientes son los más comunes:

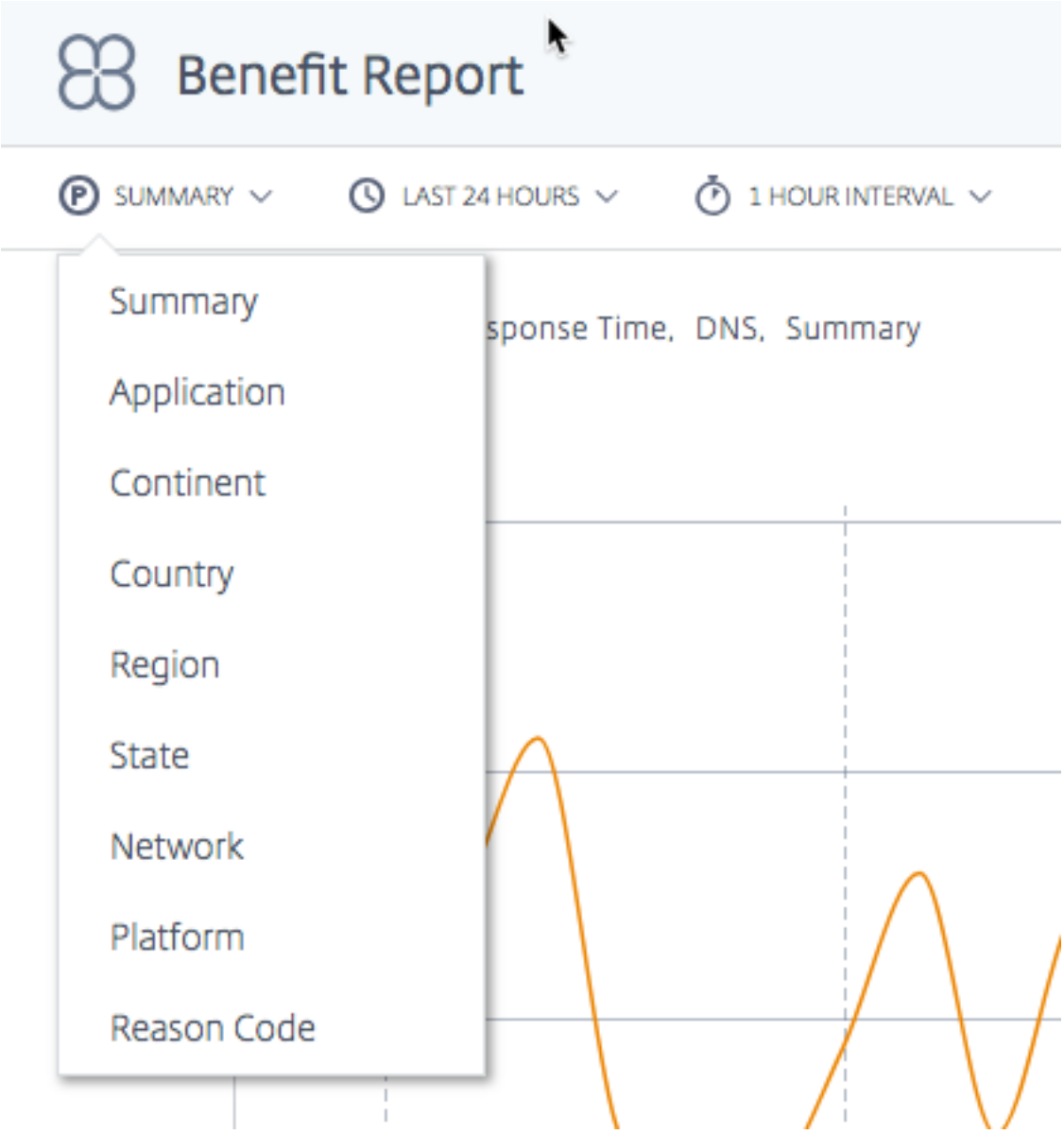
- **Estadística** - Seleccione el valor mostrado en el gráfico, la mayoría de las veces el número de decisiones.
- **Origen del tráfico**: Seleccione el tipo de tráfico que quiere mostrar: DNS o HTTP.
- **Aplicación**: Seleccione una o más aplicaciones Openmix para mostrar.
- **Plataforma**: Seleccione una o más plataformas (proveedor) para incluir.
- **Continente**: Seleccione uno o más continentes para incluir.
- **País**: Seleccione uno o más países para incluir.
- **Región**: Seleccione una o más regiones geográficas (cuando corresponda) que quiera incluir.
- **Estado**: Seleccione uno o más estados geográficos (cuando corresponda) para incluirlos.
- **Red**: Seleccione una o más redes (ASN) que quiere incluir.

Informe de beneficios

El informe Benefit le ofrece la mejora general del rendimiento de la entrega de aplicaciones cuando utiliza el servicio NetScaler Intelligent Traffic Management (ITM). El beneficio se muestra como un porcentaje de mejora en el tiempo de respuesta y el rendimiento. Elija una plataforma específica del grupo de plataformas candidatas para generar el informe.

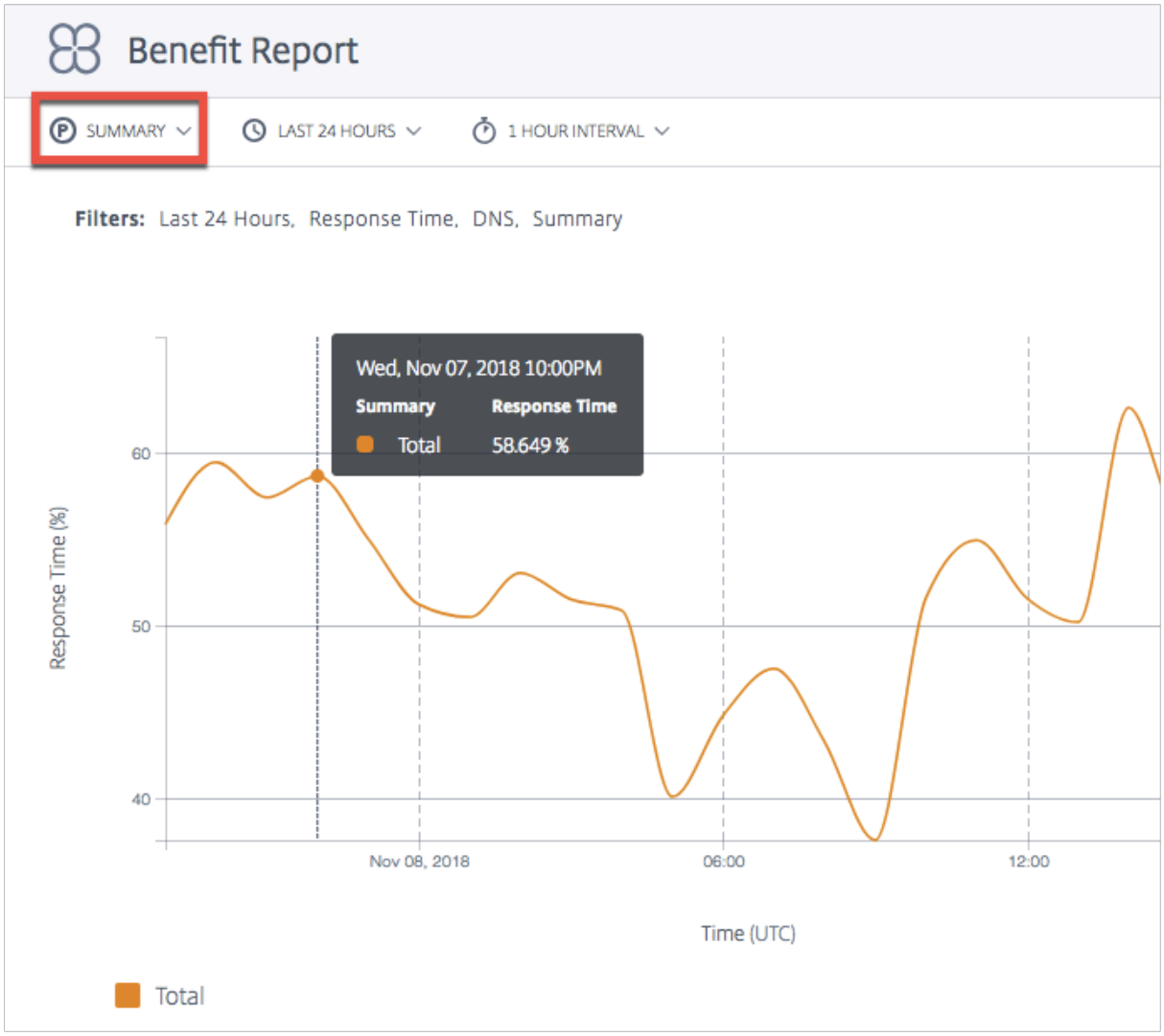
Dimensiones principales del informe Benefit

Las dimensiones principales son medidas independientes basadas en las que se muestra el informe de beneficios. En las secciones siguientes se describen detalladamente cada una de estas dimensiones principales.



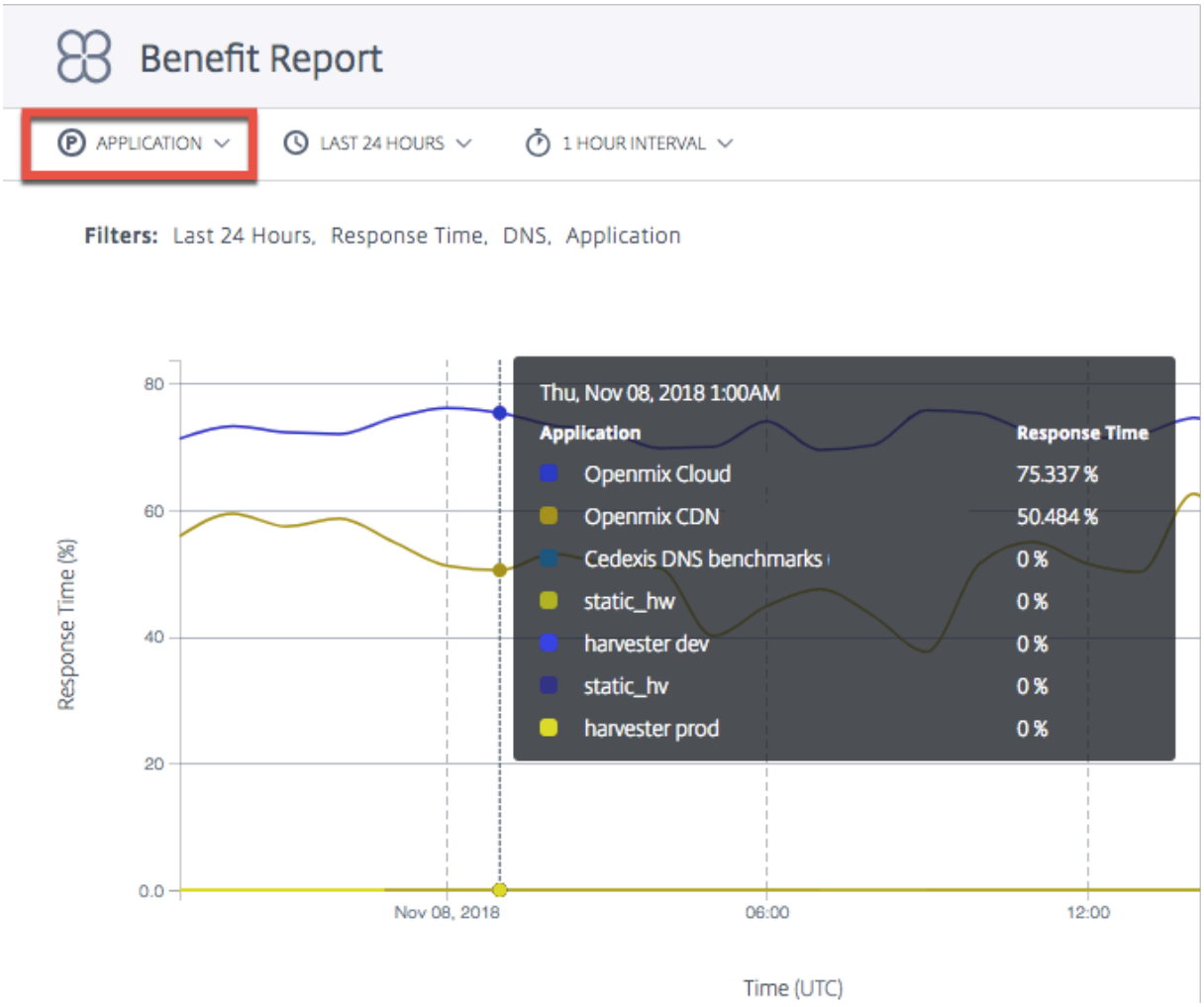
Resumen **Resumen** es la dimensión principal predeterminada. El gráfico de resumen muestra el promedio del porcentaje total de beneficio (en términos de tiempo de respuesta o rendimiento) recibido de todas las aplicaciones.

Nota: Puede cambiar entre el beneficio mostrado en términos de **tiempo de respuesta**o **rendimiento**mediante el filtro de **estadísticas**.



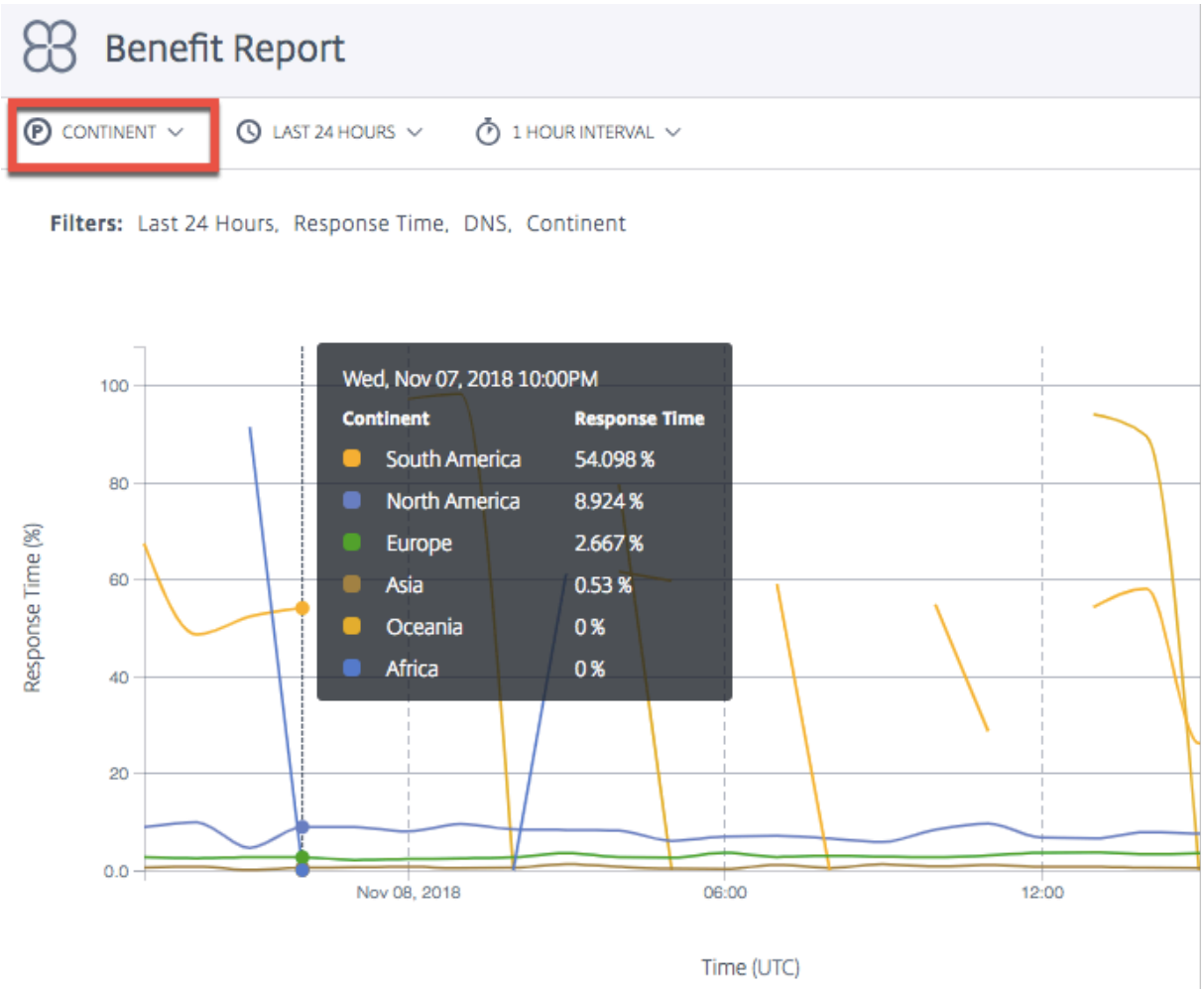
Aplicación Cuando se elige la **aplicación** como dimensión principal, el gráfico muestra cada una de las aplicaciones y el rendimiento correspondiente (en términos de tiempo de respuesta o rendimiento) como un beneficio porcentual al elegir una plataforma determinada sobre otras plataformas candidatas.

Nota: 0% significa que no hubo ningún beneficio o mejora adicional al seleccionar una plataforma específica en lugar de otra.

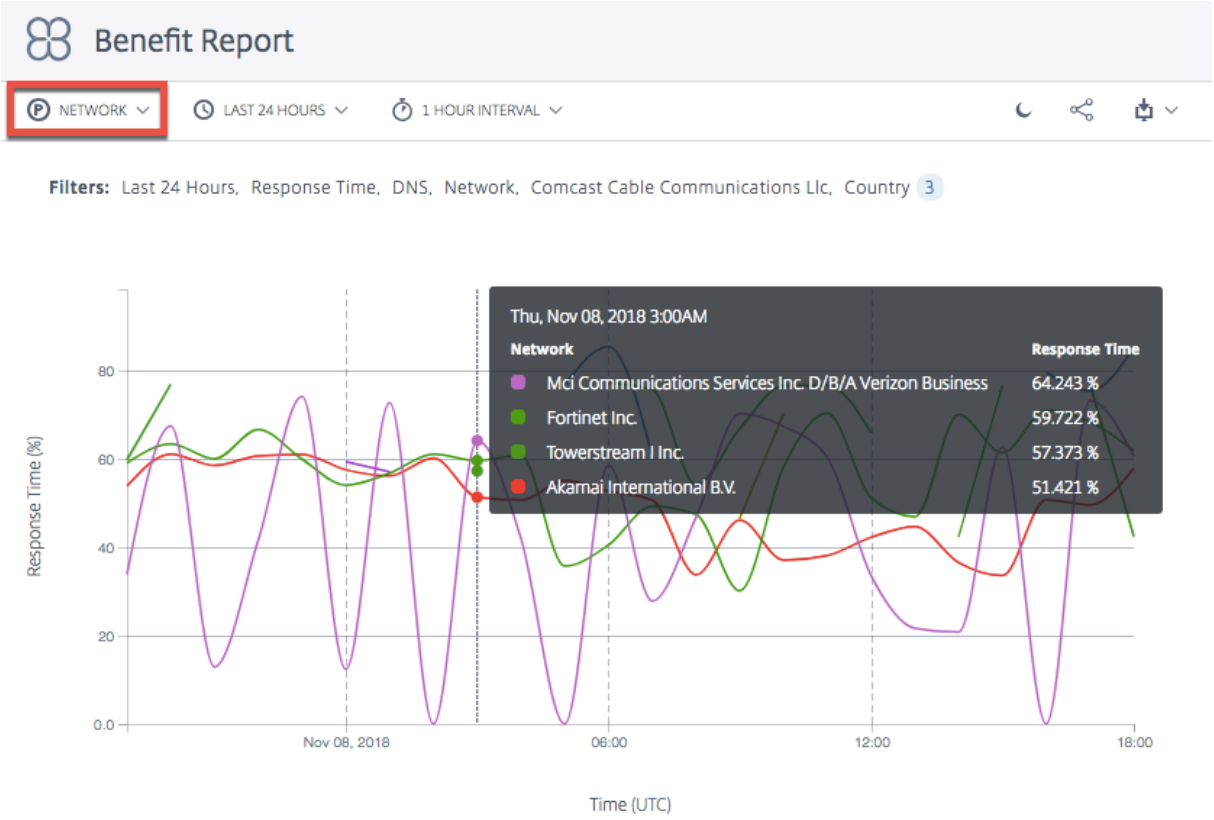


Ubicación (Continente, País, Región, Estado) Cuando se selecciona la ubicación (**Continente**, **País**, **Región**o **Estado**) como dimensión principal, el informe de beneficios muestra el promedio del porcentaje total de mejora en rendimiento (en términos de tiempo de respuesta o rendimiento) para cada ubicación. Puede seleccionar la ubicación por continente, país, región o estado.

Nota: Las plataformas que no son aptas para la selección debido a reglas geográficas o cualquier otra razón no se incluyen en el cálculo. Sin embargo, se cuentan las plataformas que están geo-cercadas para la ubicación en cuestión.

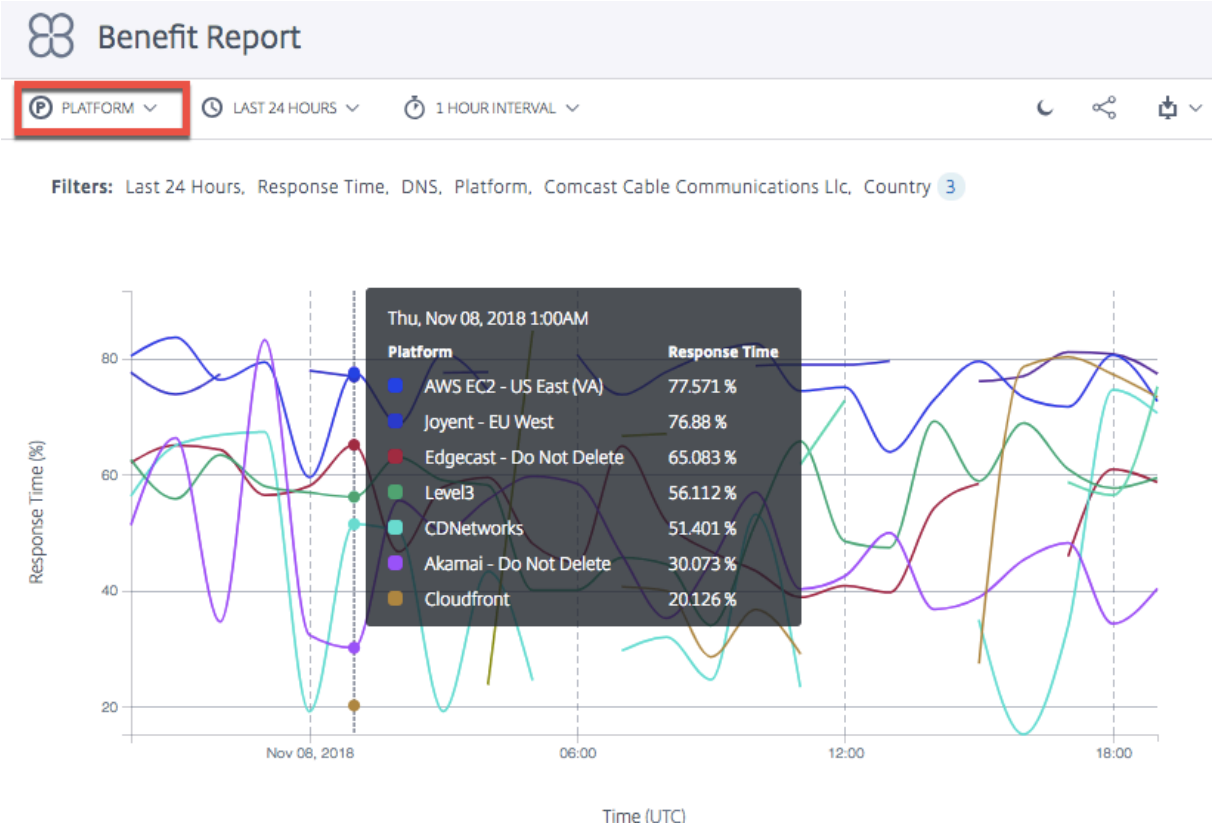


Red Al seleccionar **Red** como dimensión principal, verá el porcentaje de mejora en el rendimiento de los usuarios agrupados en redes específicas (o proveedores de servicios) desde las que los usuarios acceden a ITM. Le ayuda a saber qué grupos de usuarios están viendo el beneficio de rendimiento cuando provienen de esas redes específicas.

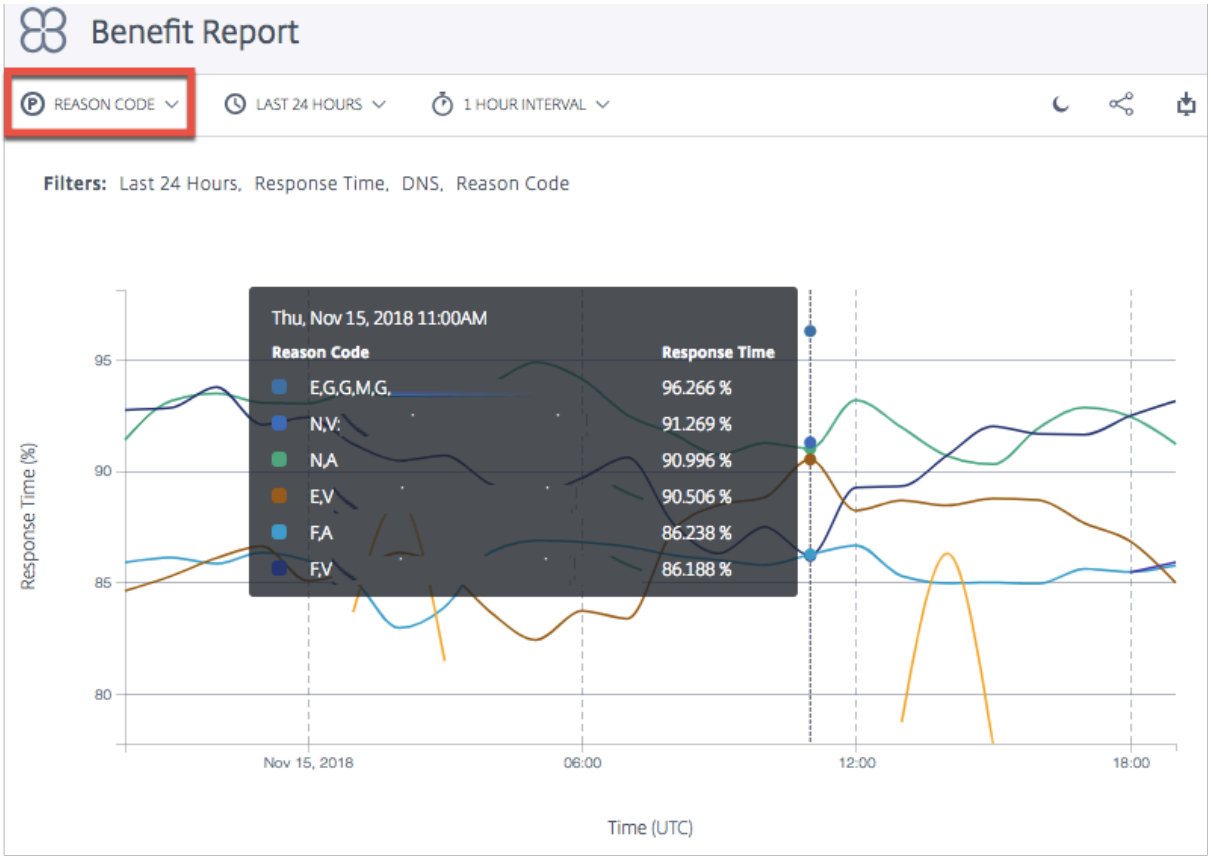


Plataforma Cuando selecciona **Plataforma** como dimensión principal, verá las plataformas individuales elegidas por diferentes aplicaciones y el rendimiento mejorado correspondiente cuando se eligen. El rendimiento o beneficio mejorado es en términos de tiempo de respuesta o rendimiento (en porcentaje).

Nota: El porcentaje de mejora en el rendimiento que se muestra cuando una aplicación elige esa plataforma. La lista del gráfico no indica necesariamente una clasificación de rendimiento entre estas plataformas.



Código de motivo Al seleccionar **Código de motivo** como dimensión principal, el porcentaje mostrado en el gráfico es el beneficio promedio general cuando se toman decisiones para un código de motivo específico.



Ignorar plataformas en el informe de beneficios

Para mejorar la precisión de las decisiones de **Openmix** para su informe de beneficios, puede optar por ignorar ciertas plataformas y configurar la aplicación para que solo seleccione las plataformas más adecuadas para la comparación.

Por ejemplo, su aplicación tiene cinco plataformas a considerar para la comparación: tres en Europa para el tráfico europeo y dos en Estados Unidos para el tráfico estadounidense. Las reglas geográficas especifican que el tráfico europeo debe pasar por las plataformas europeas y el tráfico estadounidense a través de las plataformas estadounidenses.

Para garantizar que el cálculo se realice utilizando las tres plataformas europeas, puede configurar la aplicación para que ignore las otras dos plataformas no europeas. Usa el método `ignoredProvider()` en su JavaScript.

El método toma el alias del proveedor (por ejemplo`provider-1`,`provider-2`) como argumento de entrada (al igual que el método requireProvider ()). La API debe llamarse una vez por alias.

Use este código de ejemplo en su archivo JavaScript dentro de la función `onRequest`:

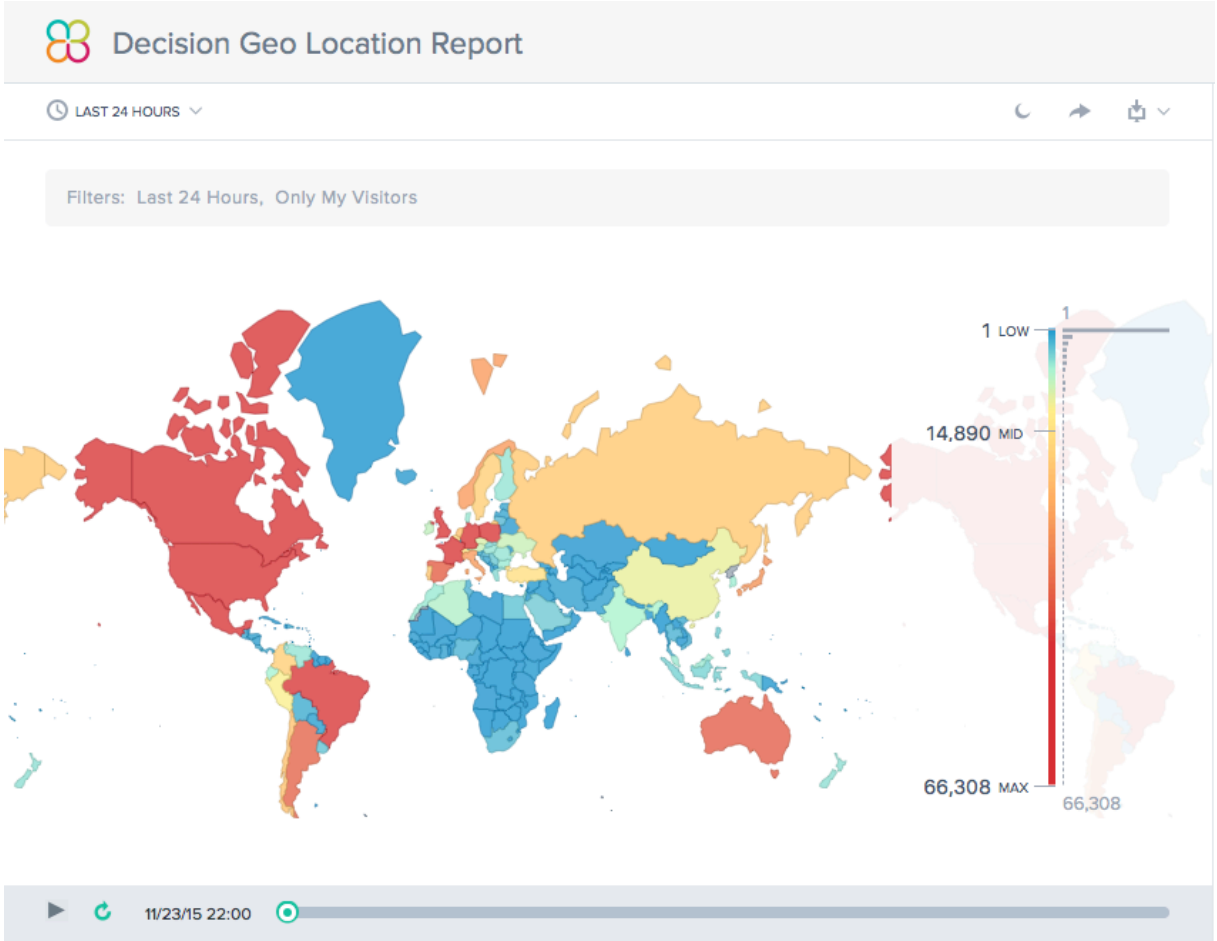
```
function onRequest(request, response) {

```



```
3    response.ignoredProvider('provider-1');
4    response.ignoredProvider('provider-2');
5    response.setReasonCode('Ignoring provider-1 and provider-2');
6    response.setTTL(this.__defaultTTL);
7    response.respond('provider-3', 'cmg.test.fake.cname');
8   }
9
10 <!--NeedCopy-->
```

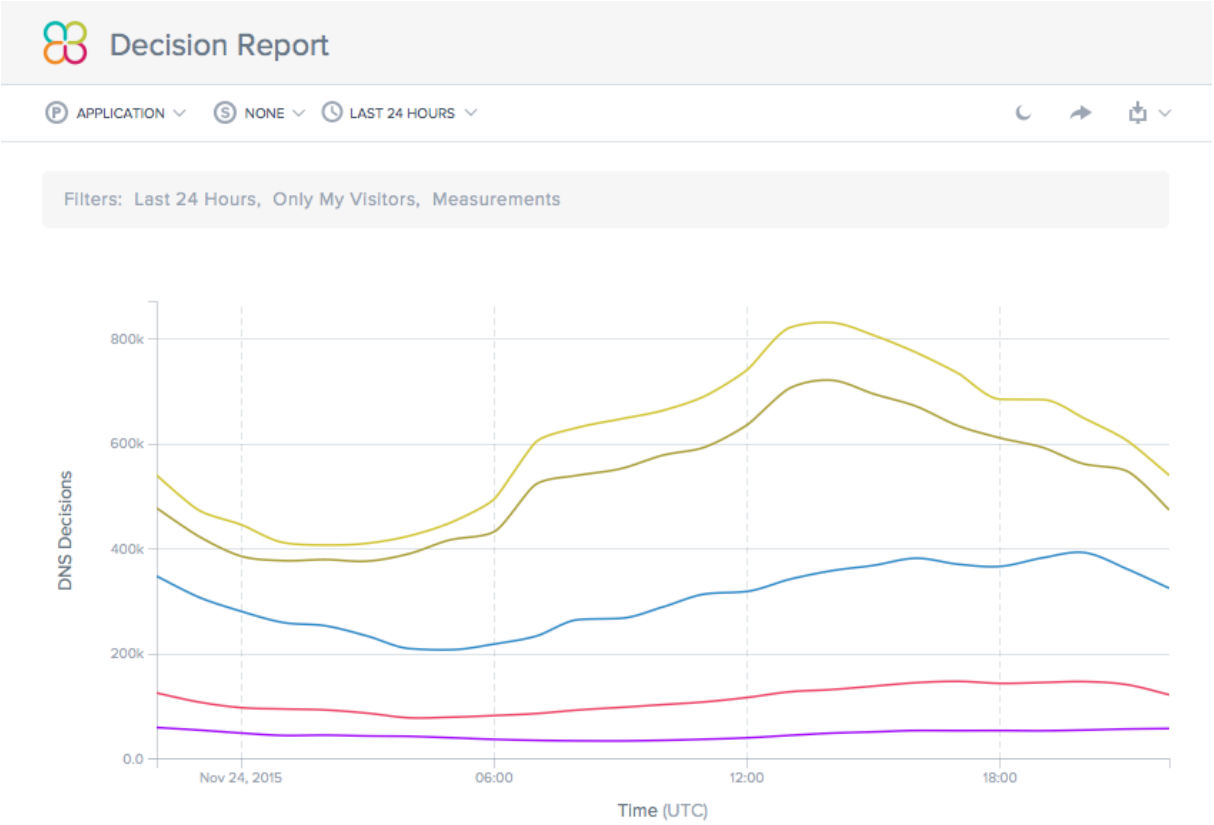
Informe de ubicación geográfica de la decisión

Este informe muestra el volumen de decisiones de Openmix para cada país. Esta vista de mapa se puede ver a lo largo del tiempo (según el intervalo de tiempo elegido para el informe) seleccionando el botón **Reproducir** en la parte inferior del gráfico.



Informe de decisión

Este informe muestra la tendencia de las decisiones de Openmix para cada una de las aplicaciones, plataformas y geografías.



DNS predictivo

September 13, 2023

Introducción

El DNS predictivo es una plataforma DNS autorizada basada en aprendizaje automático que administra las zonas y toma decisiones de enrutamiento en función de la disponibilidad del servicio en tiempo real. Está altamente disponible, con múltiples redes Anycast, que proporcionan reglas de enrutamiento flexibles y confiables. Es una oferta empresarial para clientes DNS sofisticados que valoran la calidad de su proceso de toma de decisiones DNS. Es para clientes que necesitan ejecutar una directiva de gestión de tráfico global basada en datos, inteligente y basada en una infraestructura robusta y de alto rendimiento.

El DNS predictivo admite la creación de zonas principal y secundaria. La importación de zonas también se admite con los tipos de registro más utilizados, como A (versión IPv4), AAAA (versión IPV6), NS, SOA, CNAME, MX, PTR, SRV, SPF y TXT. También apoyamos a los clientes de Openmix con una

integración perfecta a través de registros de aplicaciones Openmix. Cualquier número de registros A/AAAA/CNAME en una zona se puede hacer completamente inteligente Openmix en cualquier punto. Los clientes también pueden ejecutar DNS predictivo en un entorno principal dual usando nuestra API para impulsar la configuración.

Aspectos destacados de la integración predictiva de DNS y Openmix

1. Transición sin problemas entre registros estáticos y una sofisticada directiva de administración de tráfico basada en datos con cero downtime.
2. Directivas de administración de tráfico totalmente configurables (round robin, distribuido, basado en la geografía, basado en la red, etc.).
3. Se ha agregado conocimiento de datos en tiempo real del tráfico global de Internet, el estado de los dispositivos de punto final, el estado de la infraestructura, el estado de los proveedores de terceros, etc.
4. Fácil de aprovisionar o modificar la gestión del tráfico.
5. Análisis profundo e informes sobre la actividad de solicitud.

Pasos para configurar y delegar una zona

Antes de iniciar sesión en el portal de administración inteligente del tráfico de NetScaler, estos son algunos pasos de alto nivel que le ayudarán a comprender cómo configurar y delegar una zona.

Paso 1: Define y crea tu zona

Para empezar, cree una zona con el mismo nombre que el nombre de dominio de su empresa.Una zona representa un único dominio principal con una colección de registros dentro de él. Proporciona información sobre cómo desea enrutar el tráfico para su dominio y sus subdominios. Si tiene un archivo de zona del proveedor DNS actual, impórtelo. Con un archivo de zona importado, puede crear rápidamente todos los registros de la zona.

Paso 2: Agregue y pruebe sus registros

Puede crear registros manualmente en la consola de DNS predictivo del portal de administración inteligente del tráfico de NetScaler o puede importar un archivo de zona con todos sus registros. Al importar un archivo de zona, el DNS predictivo replica la definición de zona original migrando todos los registros existentes dentro de él.

También puede crear zonas y registros mediante programación mediante la API DNS predictiva. La API se puede encontrar en el portal en **Mis cuentas > API > Configuración > authdns**.

Los clientes de Openmix pueden asignar una aplicación Openmix existente a un registro CNAME o A/AAAA a través del tipo de registro Openmix App. Cualquier número de registros A/AAAA/CNAME en una zona se puede hacer completamente inteligente Openmix en cualquier punto.

Para probar los registros de la zona, puede utilizar una herramienta llamada dig que consulta directamente los servidores DNS. Ejecute dig con el nombre de la zona como parámetro.Por ejemplo:

`dig @ns1.ourdomain.net NS mydomain.com`

`dig @ns1.ourdomain.net A host.mydomain.com`

`@ns1.ourdomain.net` Le indica que debe realizar una solicitud a la infraestructura DNS de NetScaler Intelligent Traffic Management, y el tipo de registro (NS o A) indica qué registro solicitar. El comando NS solicitaría los registros NS para la zona `mydomain.com`, y el segundo comando `@ns1.ourdomain.net A host.mydomain.com` sería un registro A para el host de la zona `mydomain.com`.

Paso 4: Asigne NetScaler Intelligent Traffic Management como DNS autorizado actualizando sus servidores de nombres

Para asignarnos como DNS autorizado para administrar su nombre de dominio, actualice los servidores de nombres que son responsables de responder a sus consultas DNS a nuestros servidores de nombres. El nuevo servidor de nombres ITM de NetScaler responderá entonces con autoridad en nombre de su empresa.

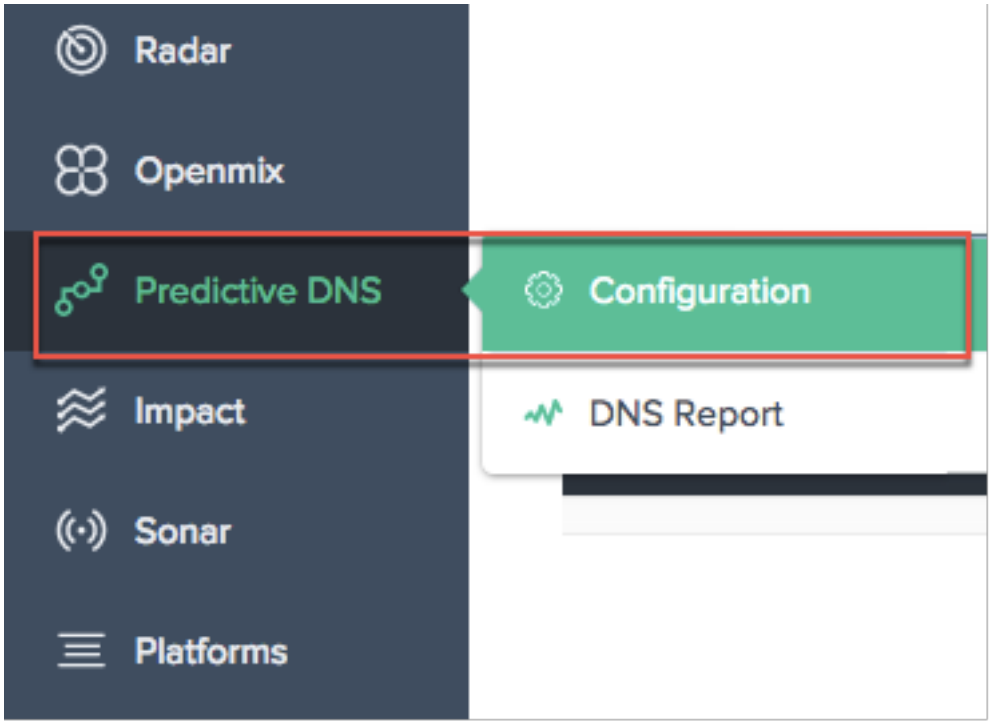
Paso 5: Validar el flujo de tráfico apropiadamente

Inicialmente, verá tráfico en funcionamiento entre ambos sistemas (su servicio DNS anterior y Citrix Predictive DNS), dependiendo de la longitud del TTL en el sistema anterior. El tráfico puede tardar un tiempo en migrar completamente. Si experimenta algún error durante la migración, vuelva a los servidores de nombres proporcionados por el servicio DNS anterior y, a continuación, determine qué salió mal. Si ve que el tráfico fluye como se esperaba, ha migrado correctamente a Citrix Predictive DNS. El TTL predeterminado aquí es 3600 segundos. Es posible que desee reducir el TTL inicialmente hasta que se asegure de que la migración es correcta. Una vez que esté satisfecho con el flujo de tráfico, puede aumentar el TTL a una duración más larga según corresponda.

Navegación

Para navegar a la consola de DNS predictivo, haga lo siguiente:

1. Inicie sesión en el portal de administración inteligente del tráfico de NetScaler.
2. En el menú de navegación de la izquierda, elija **DNS predictivo > Configuración**.



Esto le llevará a la página **Agregar zona**, donde puede comenzar creando su zona.

Zonas primaria y secundaria

Una zona representa un único dominio principal con una colección de registros dentro de él. Puede configurar la zona en DNS predictivo como principal o secundaria. DNS primario y secundario es una forma de crear redundancia en el DNS. Primario a veces se llama maestro mientras que el secundario se llama esclavo. Esto se debe a que el primario tiene la copia maestra de los datos de zona, mientras que el secundario solo clona esos datos a través de transferencias de zona a intervalos regulares o cuando el primario lo solicita.

Este proceso también se denomina a menudo transferencia de zona o transferencia AXFR. Si configura la zona principal con transferencias de zona habilitadas, todos los cambios realizados en la zona se propagarán automáticamente a todos los servidores secundarios. Cada IP que se introduce como servidor secundario recibe esta actualización. Del mismo modo, también puede configurar una zona secundaria.

Al crear una zona, se crean automáticamente un registro de servidor de nombres (NS) y un registro de inicio de autoridad (SOA) para la zona. Puede utilizar la interfaz de usuario DNS predictivo para agregar, modificar, duplicar o eliminar zonas.

Nota: Estas operaciones (modificar, duplicar o eliminar) afectan a toda la zona, incluidas todas las respuestas de cualquier registro dentro de la zona. Deben hacerse con extrema precaución.

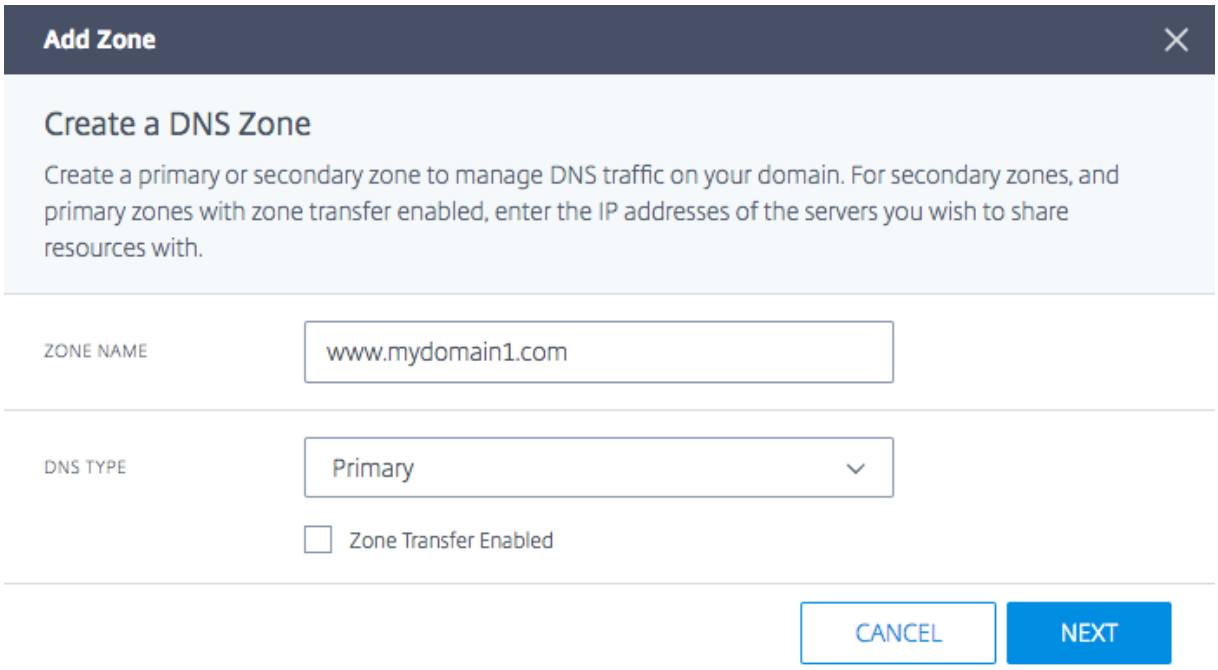
Agregar zona

Para agregar o crear una zona:

1. Si esta es tu primera vez, aparece la pantalla de inicio donde puedes hacer clic en **Agregar zona** para empezar.
2. Esto le lleva al cuadro de diálogo **Agregar zona**, donde puede crear una zona para su dominio.

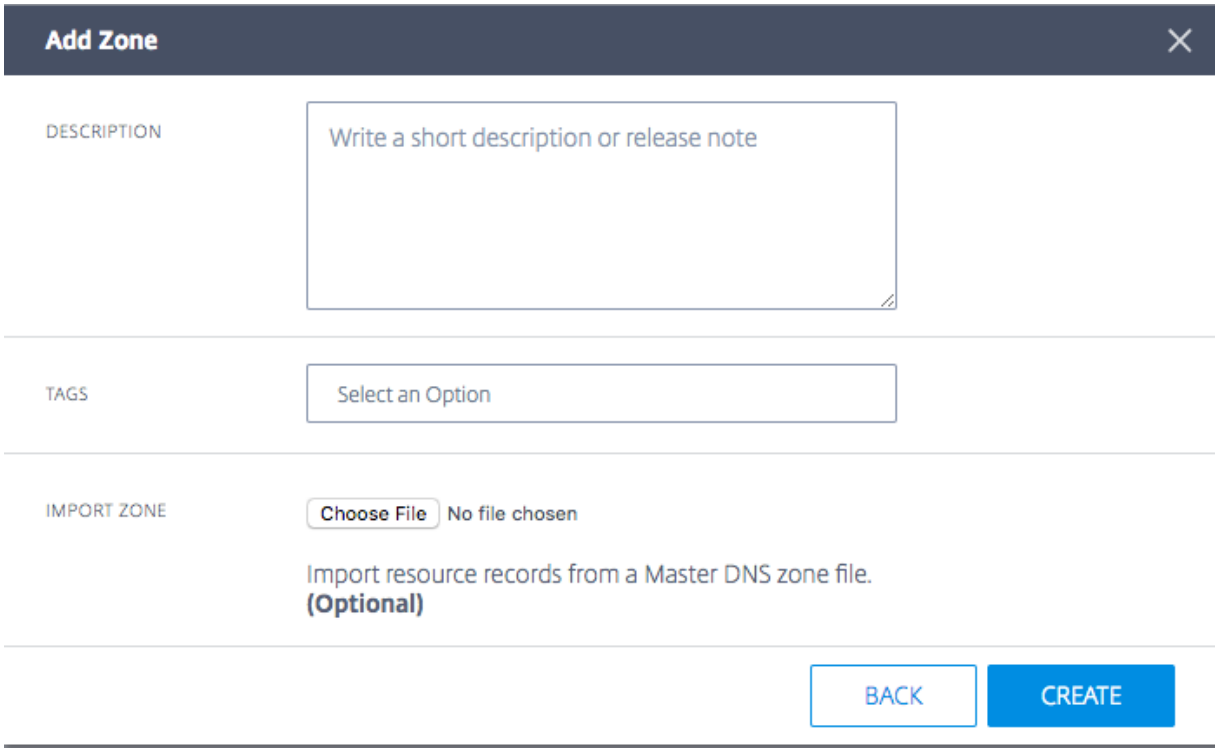
Si no es la primera vez, verá una lista de zonas existentes (nombres de dominio) creadas para los dominios de su empresa y el número de registros asociados a cada uno de ellos.

1. Haga clic en el icono de agregar en la parte superior derecha de la página para empezar a crear una zona.
2. Se abrirá el cuadro de diálogo **Agregar zona**.



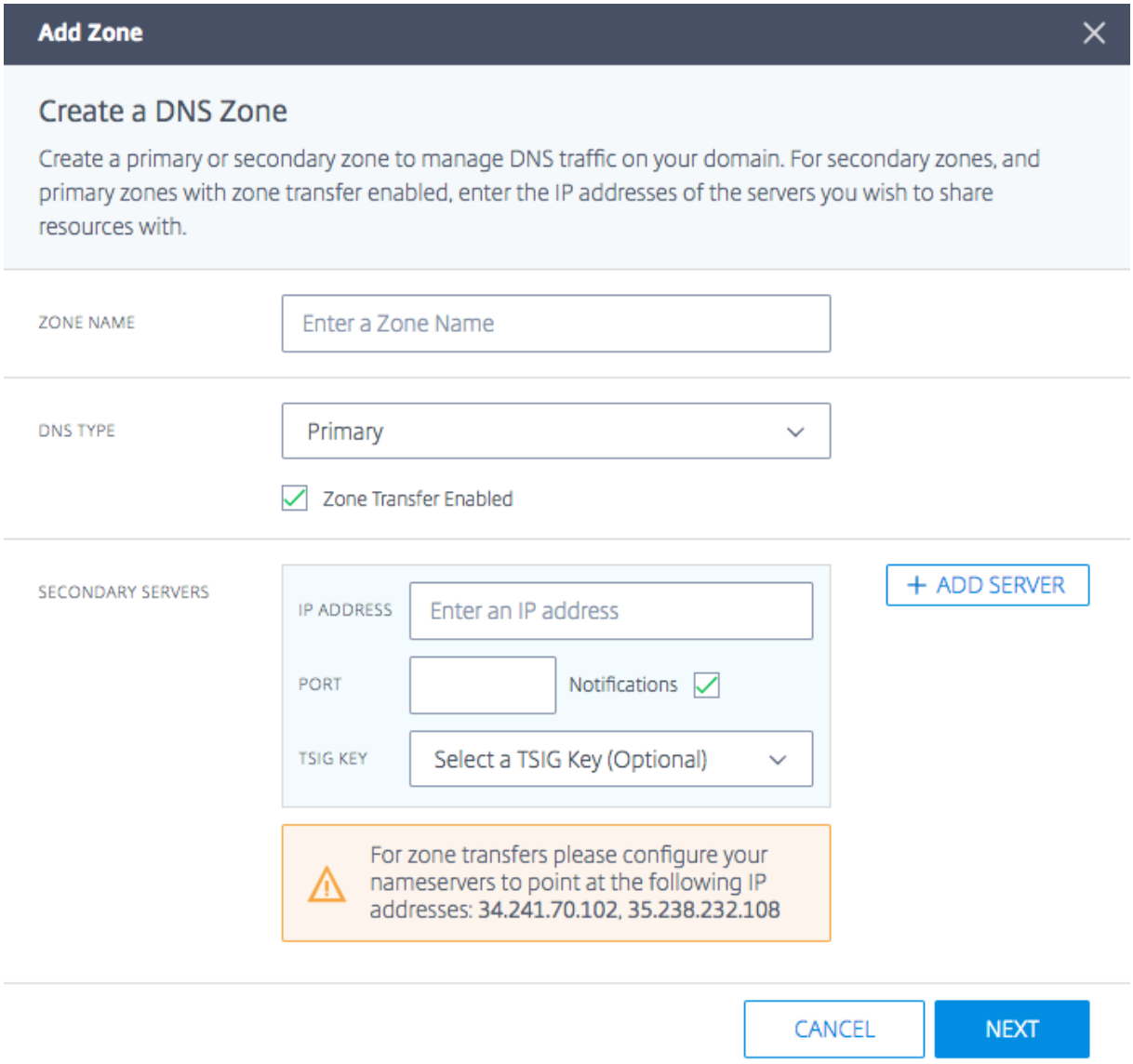
1. Introduzca su nombre de dominio como **Nombre de zona**. Por ejemplo`www.mydomain.com`. El nombre de la zona debe ser global único, lo que significa que no se puede crear un nombre de zona que exista o incluso se superponga parcialmente con un nombre de zona existente. Sin embargo, si hay una situación válida en la que necesitas crear un nombre de zona que pueda superponerse con uno existente, o si no puedes crear una zona para un dominio de tu propiedad, ponte en contacto con el servicio de asistencia.
2. Seleccione el **tipo DNS** como **Principal** o **Secundario**.
3. Haga clic en la casilla de verificación **Transferencia de zona habilitada** para habilitar la transferencia de zona e introduzca información para el servidor **primario** o **secundario**. Consulte la información del servidor para obtener más información.

4. Haga clic en **Siguiente** para introducir información de zona, como una **descripción** y **etiquetas**.
5. Seleccione **Elegir archivo** para importar un archivo de zona desde su equipo (si está disponible).
6. Haga clic en **Crear** para completar la adición de una nueva zona.



A medida que se crean nuevas zonas, aparecen en la lista de la página **Zonas**.

Información del servidor



Dirección IP Introduzca la IP del servidor primario o secundario.

Puerto Introduzca el número de puerto asociado al servidor. Este campo es opcional. Es configurable solo para servidores secundarios. Si se deja vacío, el valor predeterminado es 53.

Notificaciones Habilite las notificaciones marcando la casilla de verificación **Notificaciones** si desea que el DNS principal notifique al secundario cuando se produzcan actualizaciones. Si la casilla está desactivada, las actualizaciones del primario se envían al secundario en intervalos regulares de 60 minutos.

Agregar servidor El botón **Agregar servidor** le permite configurar varios servidores para transferencias de zona.

Clave TSIG Puede seleccionar una **clave TSIG** de la lista. Esta lista contiene claves que se crean y administran en la sección Teclas de TSIG. Se trata de un campo opcional para aumentar la seguridad. Consulte las claves TSIG para obtener más información.

Descripción Agregue una breve descripción o comentario sobre la zona que está a punto de crear. Este es un campo opcional, totalmente para su propio requisito. No afecta a las respuestas DNS reales de ninguna manera.

Etiquetas Las etiquetas le permiten ordenar y filtrar las zonas en una lista. Este es también un campo opcional.

Zona de importación Si tiene un archivo de importación de zona que tiene la configuración para su zona, se puede importar aquí. Para importar un archivo de zona, primero cree una zona con el mismo nombre que el archivo que está importando. Los siguientes son los requisitos para la importación:

- El nombre de la zona en el archivo de zona debe coincidir con el nombre de la zona que está creando.
- El archivo de zona utiliza un formato BIND estándar para los registros.
- El archivo importado debe tener un formato de archivo de zona definido por RFC.
- Puede importar un máximo de 5000 registros. Si necesita importar más de 5000 registros, póngase en contacto con el servicio de asistencia.

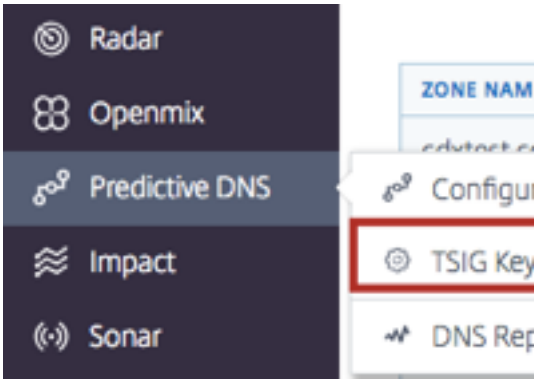
Para importar un archivo de zona, haga lo siguiente:

1. En el cuadro de diálogo **Agregar zona**, vaya a **Zona de importación**.
2. Haga clic en **Elegir archivo**.
3. Seleccione el archivo de zona que desea utilizar para rellenar la zona.
4. Haga clic en **Crear** para completar el proceso.

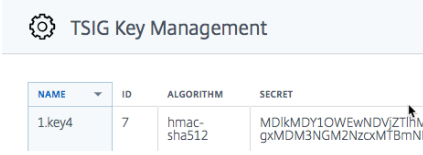
Teclas TSIG

Las claves TSIG proporcionan un nivel adicional de seguridad para compartir información entre un servidor primario y secundario. El secreto de la clave debe estar disponible en ambos servidores (primario y secundario) para que tenga lugar un protocolo de enlace correcto.

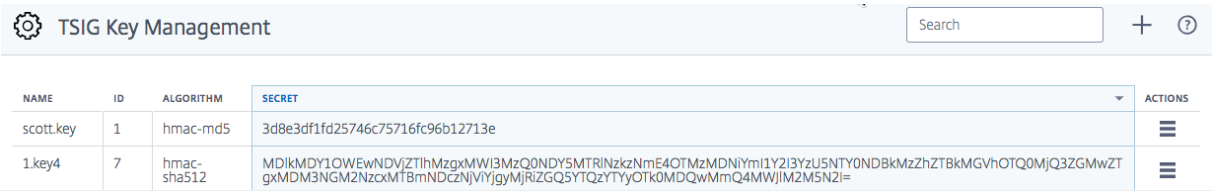
Para generar y administrar claves TSIG, haga lo siguiente:



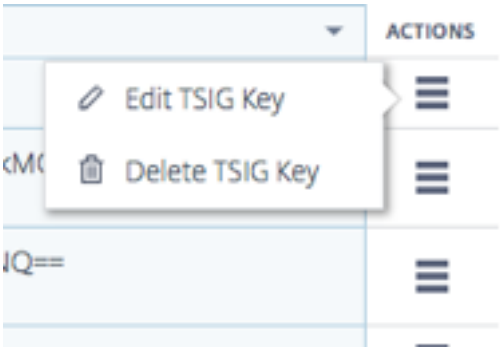
1. En el menú de navegación de la izquierda, elija **DNS predictivo**.
2. Haga clic en **Gestión de claves TSIG**.
3. Se abrirá la página Gestión de claves de TSIG.



4. Haga clic en el icono de agregar en la parte superior derecha de la página.
5. Se abrirá el cuadro de diálogo **Agregar clave TSIG**.
6. Introduzca un **nombre** para el TSIG.
7. Seleccione un algoritmo de la lista.
8. En **Secreto**, tiene la opción de introducir cualquier palabra o frase en el campo. Siempre que lo que introduzca tenga 32 caracteres (sin espacios) y codificación base64, se acepta como tal. De lo contrario, se hash de acuerdo con el algoritmo que seleccione. **Nota**: Los valores de secreto y algoritmo deben coincidir entre los sistemas primario y secundario. El valor del secreto tiene que estar codificado en base64 y tener una longitud de carácter de 32 caracteres. El botón Generar hash solo está ahí para ayudar a generar un hash si uno no existe ya.
9. Haga clic en **Crear** para completar la generación de la clave. El TSIG recién creado aparece en la página **Gestión de claves de TSIG**.

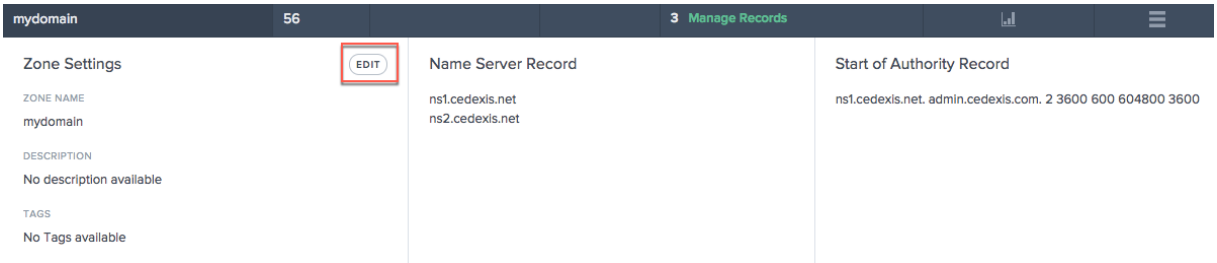


Para modificar o eliminar la clave **TSIG**, haga clic en la columna **Acciones**. Elija **Modificar** para modificar o **Eliminar** para eliminar la clave.



Modificar zona

1. Haga clic en el nombre de la zona que desea modificar.
2. Se abrirá el cajón de edición.
3. Haga clic en el botón **Modificar** para realizar cambios en el nombre de la zona, la descripción y las etiquetas.
4. Haga clic en **Save** para guardar los cambios.

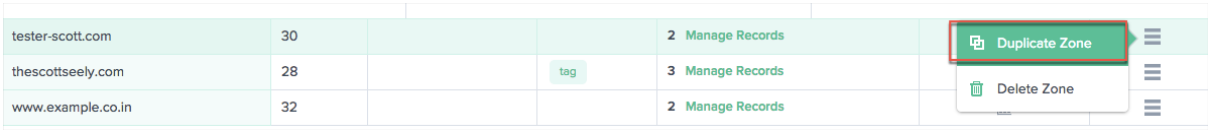


Importante: Tenga cuidado al modificar un nombre de zona. Dado que todos los registros de la zona tienen efectivamente sufijos con el nombre de la zona, el cambio de nombre de una zona cambia cada solicitud.

Zona duplicada

Duplicar una zona significa simplemente crear otra zona con información de una zona existente, pero con un nombre de zona diferente.

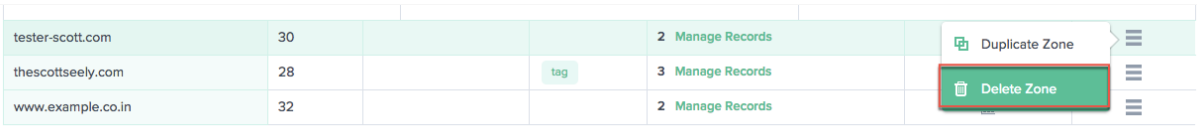
1. Para duplicar una zona, haga clic en el icono de la columna **Acciones**.
2. Seleccione **Duplicar zona**.
3. Se abre el cuadro de diálogo **Agregar zona** con información de la zona original.
4. Asigne un nuevo nombre a la zona y cambie la información que necesite.
5. Haga clic en **Crear** para completar el proceso.
6. Se crea una nueva zona con los registros y la información que se encuentran en la zona original.



Nota: Puede cambiar cualquier información dentro de la nueva zona a su discreción. Pero debe cambiar al menos el **Nombre de la zona** para crear una zona duplicada. No se permiten nombres de zona duplicados.

Eliminar zona

1. Para eliminar una zona, haga clic en el icono de la columna **Acciones**.
2. Elija **Eliminar zona**.
3. Haga clic en **Confirmar**.



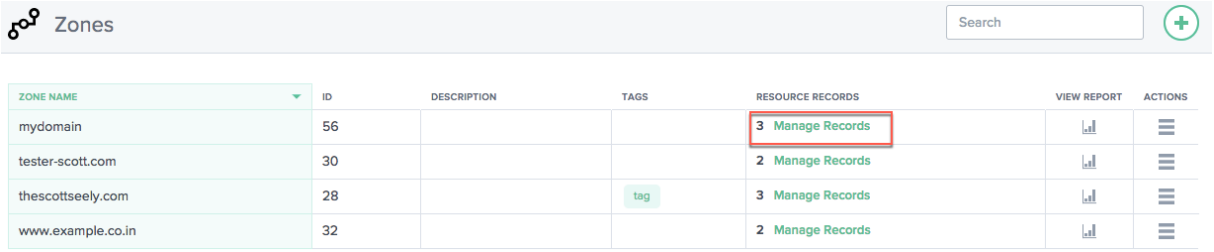
Nota de
: esta operación afecta a toda la zona, incluidas todas las respuestas de cualquier registro dentro de la zona. Esto debe hacerse con extrema precaución.

Registros

Después de crear una zona para su dominio (por ejemplo`mydomain.com`), puede agregar registros a la zona. Cada registro que agregue incluirá un nombre, un tipo de registro y otra información aplicable al tipo de registro.
Todos los registros de una zona deben tener el nombre de dominio de la zona como sufijo. Por ejemplo, si `mydomain.com` es la zona, puede contener registros con nombre, `www.mydomain.com`y, `www.portal.mydomain.com`pero no puede contener un registro denominado `www.mydomain.co.in` es decir, el nombre de cada registro se anexa con el nombre de la zona.
Nota: Cuando se crea una zona, los tipos de registro Servidor de nombres (NS) y Inicio de autoridad (SOA) se crean automáticamente para esa zona.

Administrar registros

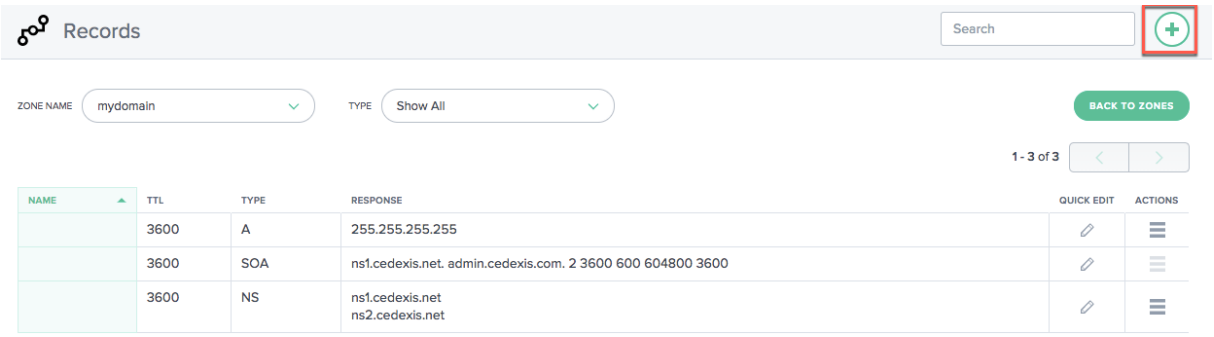
Para acceder a la página Registros y administrar los registros, haga clic en **Administrar registros** en la columna **Registros de recursos** de la zona. Se abre la página **Registros** con una lista de registros bajo la zona seleccionada. Aunque aún no haya creado ningún registro, verá al menos dos tipos de registros en Registros de recursos para una o más zonas que haya creado. Estos son los registros NS y SOA que se crean de forma predeterminada al crear la zona por primera vez.



Esta página le permite agregar, modificar, eliminar o duplicar registros. También enumera el TTL, el tipo de registro y la respuesta para cada subdominio o registro.

Agregar registro

1. En la página **Zonas**, haga clic en **Administrar registros**. Esto le lleva a la **página Registros**.
2. Para agregar un nuevo registro, haga clic en el botón Agregar en la esquina superior derecha de la página **Registros**.
3. Se abrirá el cuadro de diálogo **Agregar registro**.



Nombre Introduzca el nombre del registro. Si deja este campo vacío, se crea un registro en el vértice de la zona.Por ejemplo, si su zona es`mydomain.com` y desea un registro A en la raíz de este dominio, debe especificarlo como un registro sin nombre en la`mydomain.com` zona. Algunas otras especificaciones y proveedores se refieren a esto como el registro @.

TTL Escriba un valor para TTL.TTL es la cantidad de tiempo, en segundos, que desea que los solucionadores recursivos DNS almacenen en caché la información sobre este registro. Si especifica un valor más largo (por ejemplo, 172.800 segundos o dos días), los solucionadores reutilizarán una respuesta anterior y enviarán solicitudes al servidor DNS autorizado con menos frecuencia. Sin embargo, esto significa que los cambios en el registro tardan más en surtir efecto porque los solucionadores recursivos utilizan los valores de su caché durante períodos más largos en lugar de solicitar la información más reciente.

Tipo Seleccione el tipo de registro que desea crear. Para obtener más información sobre los distintos tipos de registros, consulte la sección Tipos de registros .

Tipo de respuesta Introduzca una respuesta adecuada para el valor del tipo de registro. Para todos los tipos excepto CNAME, puede introducir más de un valor de respuesta. Introduzca varios valores de respuesta haciendo clic en el icono de agregar. Si se introducen varios valores, se devolverán todas las respuestas especificadas para cada solicitud de ese tipo y nombre.

Haga clic en **Crear** para agregar el registro. El registro recién agregado se propaga a los servidores DNS y se sirve en vivo cuando se realiza el cambio.

Lista de registros

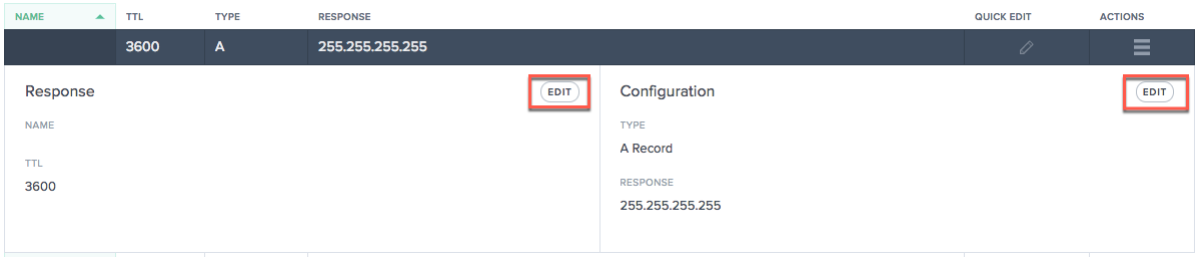
Cuando agrega un nuevo registro, aparece en la página Registros. Esta página muestra todos los registros creados bajo un **nombre de zona** específico junto con el **TTL**, el **tipo de registro** y la **respuesta** para ese registro.

Todos los registros de esta página pertenecen a una zona específica que se muestra en la lista **Nombre de zona** en la parte superior izquierda de la página **Registros**. Esta lista tiene una lista de las zonas ya creadas para su empresa. Puede cambiar a una zona diferente (y ver sus propios registros) seleccionándola en la lista.

También puede utilizar la lista **Tipo de registro** para filtrar esta lista según el tipo de registro.

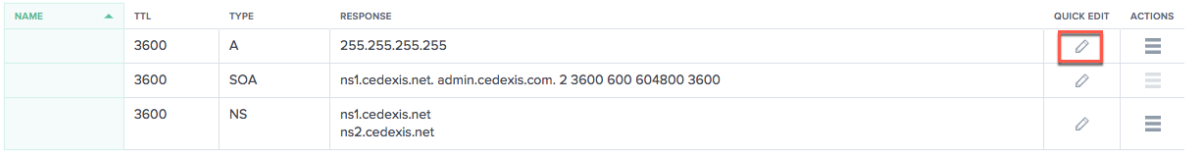
Modificar registro

Hay dos formas de modificar registros: edición detallada y edición rápida. Para realizar una edición detallada, haga clic en el registro en la lista (en la página **Registros**).Se abre para mostrar los detalles del registro con botones para modificar. Haga clic en el botón **Modificar** para mostrar la información del registro. Una vez que haya terminado de modificar, haga clic en **Guardar**para guardar los cambios.



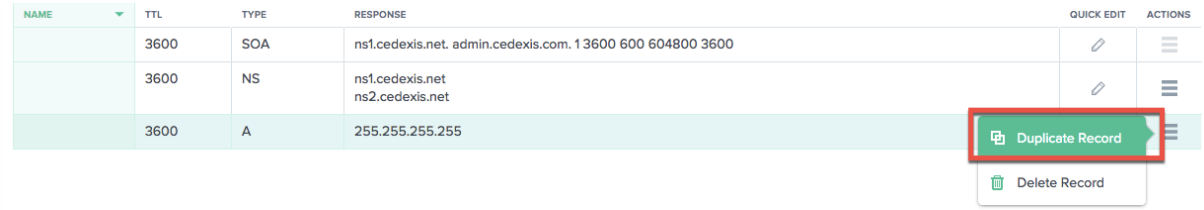
Para utilizar **Edición rápida**, simplemente haga clic en el icono de **edición (en la columna Edición rápida**) del registro que desee modificar. Usted será capaz de modificar el TTL y la Respuesta para el

registro. Cuando haya terminado de modificar, haga clic en el icono Guardar (marca de verificación) para guardar las ediciones o cancelarlas para deshacer las ediciones.



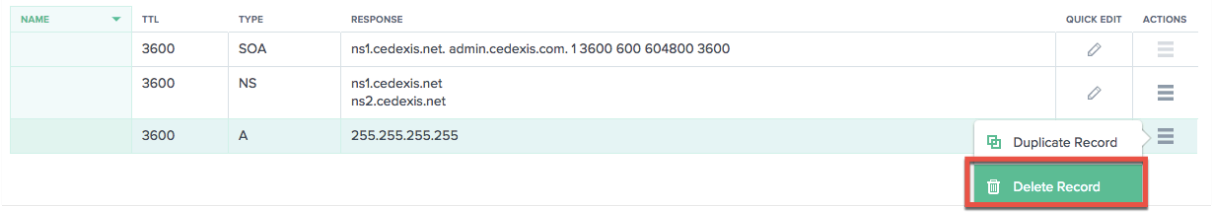
Duplicar registro

Para duplicar un registro, haga clic en el icono de la columna **Acciones**. Elija Duplicar registro. Se abre el cuadro de diálogo Agregar registro con información del registro que desea duplicar. Haga clic en Crear para crear un registro con información del registro original. Tenga en cuenta que al menos se debe cambiar el nombre o el tipo de registro para que se cree el nuevo registro.
Nota: Los registros SOA no se pueden duplicar.



Eliminar registro

Para eliminar un registro, haga clic en el icono de la columna **Acciones**. Elija Eliminar registro. Esta acción elimina el registro y el DNS predictivo ya no responderá a las consultas del registro. Para eliminar respuestas específicas de un registro, utilice la opción Edición rápida



Nota: Los registros NS y SOA son tipos de registro predeterminados y no se pueden eliminar. Estos registros se eliminarán solo si se elimina la zona misma.

Tipos de registros

Registro NS

Los registros NS o Servidor de nombres son responsables de delegar una zona DNS en un servidor autorizado. Creamos un registro de servidor de nombres (NS) que se asigna automáticamente al crear una zona, por ejemplo, ns1.ourdomain.net y ns2.ourdomain.net. Estos son los servidores de nombres que configuraría en el registrador para que las consultas DNS se puedan enrutar a su zona.
Estos servidores de nombres sirven para confirmar el conjunto de servidores disponible para las solicitudes de servicio de la zona, asegurando que el conjunto de servidores de nombres devuelto en la solicitud de delegación y por el servidor delegado coincidan. También puede modificar los servidores de nombres para asegurarse de que coincidan.

También le permitimos modificar los servidores de nombres que cree para que pueda apuntar cualquiera de sus dominios a los servidores de nombres de otra empresa que puedan contener su zona DNS y administrar sus registros allí.

Nota: Los registros NS se pueden modificar pero no se pueden eliminar.

Registro SOA

El registro Inicio de autoridad (SOA) identifica la información autorizada sobre la zona. Un registro de recursos SOA se crea de forma predeterminada al crear la zona. Puede modificar el registro según sea necesario.

Nota: Los registros SOA no pueden ser creados por el usuario, pero ciertos parámetros pueden ser editados.

El formato de un registro SOA es el siguiente: `[MNAME] [RNAME] [Serial Number] [Refresh Time] [Retry Interval] [Expire Time] [Minimum TTL]`

He aquí un ejemplo: `ns1.ourdomain.net admin.mydomain.com.314 3600 600 604800 10`

Los elementos del registro SOA incluyen:

- **MNAME**: El nombre de dominio del servidor de nombres principal, como `ns1.ourdomain.net` en el ejemplo anterior.
- **RNAME**: La dirección de correo electrónico del administrador en un formato con el símbolo @ reemplazado por un punto, como `admin.mydomain.com` en el ejemplo anterior.
- **Número de serie**: Número de revisión que se incrementará al cambiar el archivo de zona y distribuir los cambios a los servidores DNS. Un entero sin signo de 32 bits, como 314 en el ejemplo anterior.

- **Tiempo de actualización**: Tiempo de actualización en segundos que los servidores DNS esperan antes de consultar el registro SOA para comprobar si hay cambios. Intervalo de tiempo entero sin signo de 32 bits en segundos, como 3600 en el ejemplo anterior.
- **Intervalo de reintento**: Intervalo de reintento en segundos que espera un servidor secundario antes de volver a intentar una transferencia de zona fallida, como 600 (10 minutos) en el ejemplo anterior. Normalmente, el tiempo de reintento es menor que el tiempo de actualización.
- **Tiempo de caducidad**: El tiempo de caducidad en segundos que un servidor secundario sigue intentando completar una transferencia de zona, como 604800 (una semana) en el ejemplo anterior.
- **TTL mínimo**: El tiempo mínimo de vida (TTL) en segundos, como 10 segundos en el ejemplo anterior.

A: Dirección IPv4

Una dirección IP en formato IPv4, por ejemplo `192.0.2.235`. El valor de un registro A es una dirección IPv4 en notación decimal punteada.

AAAA: Dirección IPv6

Una dirección IP en formato IPv6, por ejemplo `2001:0db8:85a3:0:0:8a2e:0370:7334`. El valor de un registro AAAA es una dirección IPv6 en formato hexadecimal separado por dos puntos, tal como se especifica en las representaciones de RFC 4291/5952.

CNAME: Nombre canónico

Es el nombre de dominio completo (por ejemplo, `www.mydomain.com`) que quiere que el DNS predictivo devuelva en respuesta a las consultas DNS de este registro. Un elemento de valor CNAME tiene el mismo formato que un nombre de dominio.

Importante: El protocolo DNS no le permite crear un registro CNAME para la raíz de la zona que es que no permitimos registros CNAME sin nombre. Por ejemplo, si su zona es `mydomain.com`, no puede crear un registro CNAME para `mydomain.com`. Sin embargo, puede crear registros CNAME para `www.mydomain.com`, `portal.mydomain.com` y así sucesivamente.
Además, si crea un registro CNAME para un subdominio, no puede crear ningún otro registro para ese subdominio.Por ejemplo, si crea un registro CNAME para `www.mydomain.com`, no puede crear otros tipos de registros con el nombre `www.mydomain.com`.
Nota: Si un subdominio tiene un registro de aplicación Openmix, no puede tener registros A, AAAA o CNAME en el mismo subdominio.

MX: Mail Exchange

Este es el registro utilizado en las solicitudes de enrutamiento a los servidores de correo. Por ejemplo:
`1 mail.mydomain.com`

Cada valor de un registro MX contiene dos valores:

1. La prioridad del servidor de correo, que puede ser cualquier entero de 16 bits mayor que 0.
2. El nombre de dominio del servidor de correo.

Si especifica varios servidores, el valor que especifique para la prioridad indica a qué servidor de correo desea que se enrute el correo electrónico primero, segundo, etc. Por ejemplo, si tiene dos servidores de correo y especifica valores de 1 y 2 para la prioridad, el correo electrónico siempre va al servidor con una prioridad de 1 a menos que no esté disponible. Si especifica valores de 1 y 1, el correo electrónico se enruta a los dos servidores aproximadamente igual.

Openmix (A/AAAA/CNAME)

Los clientes de Openmix Application ahora pueden tener su registro completo establecido en la zona (incluidos los registros estáticos) administrado y servido por el mismo conjunto de servicios. Esto permite a los clientes hacer que cualquiera de sus hosts Openmix sea inteligente. Por lo tanto, cada vez que un CNAME está conectado a una aplicación Openmix, se sirve con la misma capacidad basada en datos, dinámica y totalmente programable de Openmix.

Por ejemplo, puede tener varios servidores de aplicaciones web detrás de una aplicación Openmix para su registro 'www'y la aplicación Openmix decidiría con qué CNAME responder, usando su lógica inteligente incorporada.

Nota: Una aplicación Openmix puede devolver un registro CNAME, A o AAAA y, por lo tanto, no puede tener simultáneamente una aplicación Openmix con ninguno de estos tipos de registro usando el mismo nombre.

PTR: registro de puntero

Los registros PTR se utilizan para asignar una IP a un nombre de dominio, principalmente para DNS inverso. Los registros PTR configurados correctamente pueden ser importantes para escenarios de seguridad como la validación de la credibilidad de los remitentes de correo electrónico o la búsqueda DNS inversa realizada en el establecimiento de sesión SSH. Un valor de registro PTR tiene el mismo formato que un nombre de dominio. Por ejemplo: `hostname.mydomain.com`.

SPF: Marco de directivas de remitentes

Un registro SPF identifica qué servidores de correo pueden enviar correo electrónico en nombre de su dominio. Comienza por v=spf; por ejemplo: v=spf1 ip4:192.168.0.1/16-all.

SRV: Localizador de servicios

Un registro SRV es utilizado por voz sobre IP, protocolos de mensajería instantánea, descubrimiento de servicios y otras aplicaciones. Un elemento de valor de registro SRV consta de cuatro valores separados por espacios. Los tres primeros valores son números decimales que representan prioridad, peso y puerto. El cuarto valor es un nombre de dominio.

El formato de un registro SRV es:

```
[priority] [weight] [port] [domain name]
```

Por ejemplo:

```
1 10 5269 xmpp-server.example.com
```

TXT: Texto

Un registro de texto puede contener texto arbitrario y también se puede utilizar para definir datos legibles por máquina, como información de seguridad o prevención de abusos. También se utiliza a menudo para la verificación de la propiedad del dominio (por ejemplo, puede obtener un certificado, registrar herramientas de terceros para operar en nombre de su dominio, etc.).
Solo necesita contener texto, por ejemplo, Entrada de texto de muestra.

Registro predictivo (A/AAAA/CNAME)

Los registros predictivos proporcionan varias opciones de configuración para la administración global del tráfico basada en la disponibilidad del servicio en tiempo real. Los registros predictivos permiten aplicar la configuración de enrutamiento entre grupos de direcciones y definir el comportamiento individualmente para diferentes ubicaciones, redes o bloques IPS/CIDR. Este servicio combina failover y lógica de enrutamiento round robin para asegurar la mayor disponibilidad, cero downtime y una administración de tráfico fluida basada en datos en todas las plataformas.

Los clientes de DNS predictivo pueden utilizar el tipo de registro predictivo para los tipos de respuesta CNAME, A o AAAA.

Como cliente DNS predictivo, cuando agregue registros a su zona, seleccione **Predictivo (A/AAAA/CNAME)** en la lista de **Tipos de registro**.

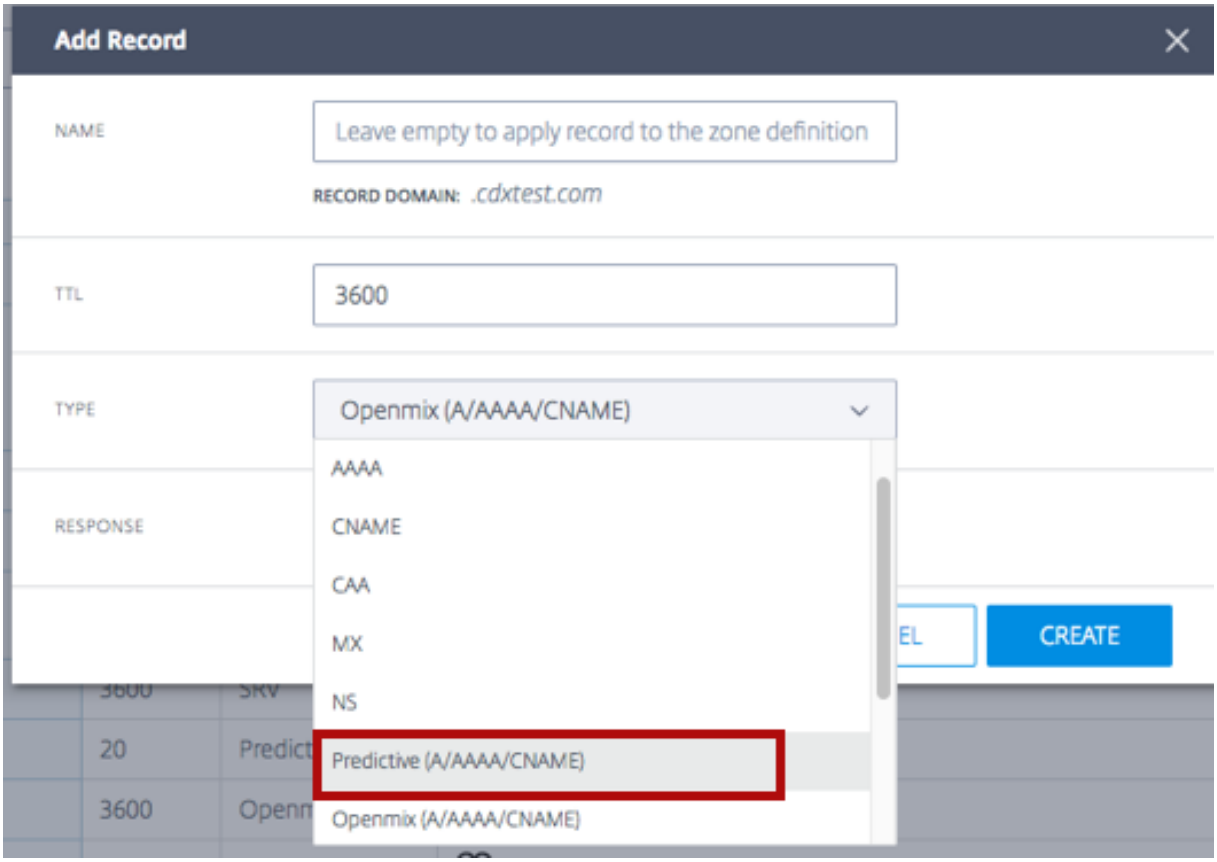
Navegación

1. Vaya a la página **Registros** de su zona.
2. Haga clic en el **botón Agregar registro** de la página Registros. Para obtener más información sobre cómo agregar registros, consulte la sección Agregar registro .
3. Se abrirá el cuadro de diálogo **Agregar registro**.

Agregar registros predictivos

En el cuadro de diálogo **Agregar registro**, escriba lo siguiente:

1. **Nombre**: Introduzca un nombre para el registro. Si se deja vacío, el registro tendrá automáticamente la definición de zona. También puede utilizar un solo asterisco (`*`) como comodín en la parte más a la izquierda del nombre para que coincida con las solicitudes de todos los subdominios inexistentes. Por ejemplo, puede utilizar `*`, `*.example.com` o `*.something.example.com`. Sin embargo, `*.` no es válido; es decir, asterisco seguido solo de un punto no está permitido. Apoyamos la funcionalidad comodín tal como se define en los RFC.
2. **TTL**: Puede dejar el TTL predeterminado tal cual, o modificarlo de acuerdo a su necesidad. **Nota:** El tiempo de vida de DNS (TTL) indica a los solucionadores cuánto tiempo deben mantener la decisión antes de solicitar actualizaciones de nuevo. El TTL se utiliza para controlar el volumen de tráfico, y también controlar la sensibilidad a los cambios en los datos sobre los que actúa. El TTL predeterminado es 20 segundos. Si baja el TTL, obtiene más volumen y más consultas DNS en tiempo real. Sin embargo, esto puede llevar a costes adicionales y un rendimiento menor (porque las consultas DNS tardan tiempo en el cliente). Por lo tanto, se recomienda no cambiar el valor predeterminado de 20 segundos.
3. **Tipo**: Haga clic en la lista **Tipo**y seleccione Predictive (A/AAAA/CNAME).
4. **Tipo de respuesta**: Haga clic en la lista **Tipo**de respuesta y seleccione su tipo de respuesta como A, AAAA o CNAME.
5. **Repliegue**: Introduzca la respuesta de **Repliegue**. Se debe especificar un CNAME, A, AAAA válido para **Fallback**. La reserva se utiliza en caso de fallo en el procesamiento de la aplicación. **Nota**: La **respuesta de reserva**debe ser un CNAME válido, si el **tipo de respuesta**seleccionado en el paso anterior es CNAME. Si el **tipo de respuesta** seleccionado es A, la respuesta de reserva debe ser una dirección CNAME o IPv4. Como alternativa, si el **tipo de respuesta** seleccionado es AAAA, la respuesta de reserva debe ser una dirección CNAME o IPv6.
6. Haga clic en **Crear y definir enrutamiento**.
7. Se abrirá la página **Configuración predictiva**.



Pasos de configuración

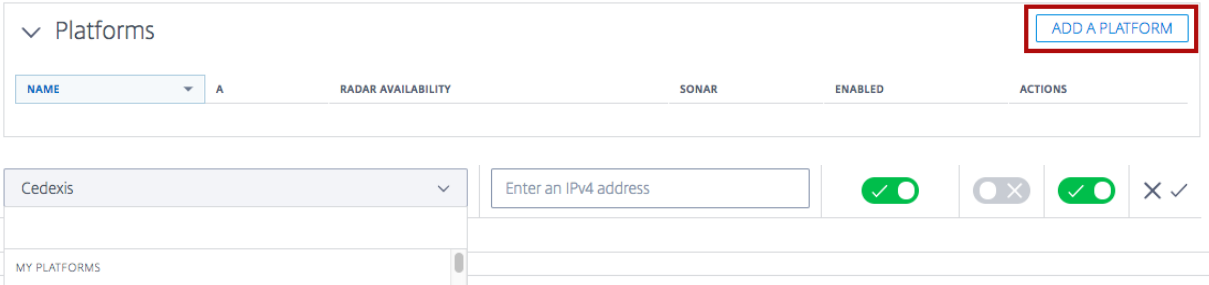
La parte superior de esta página tiene la sección **General** que muestra la configuración en el cuadro de diálogo **Agregar registro**. También tiene campos opcionales para agregar **etiquetas** o una **descripción** a los registros predictivos.

Siga los pasos que se indican a continuación para configurar el registro.

Paso 1: Elija todas las plataformas disponibles El primer paso para configurar el registro predictivo es elegir todas las plataformas que desee disponibles para diferentes ubicaciones, redes o bloques IPS/CIDR. Si no encuentra su plataforma en la lista, puede añadirla en la página Plataformas

.

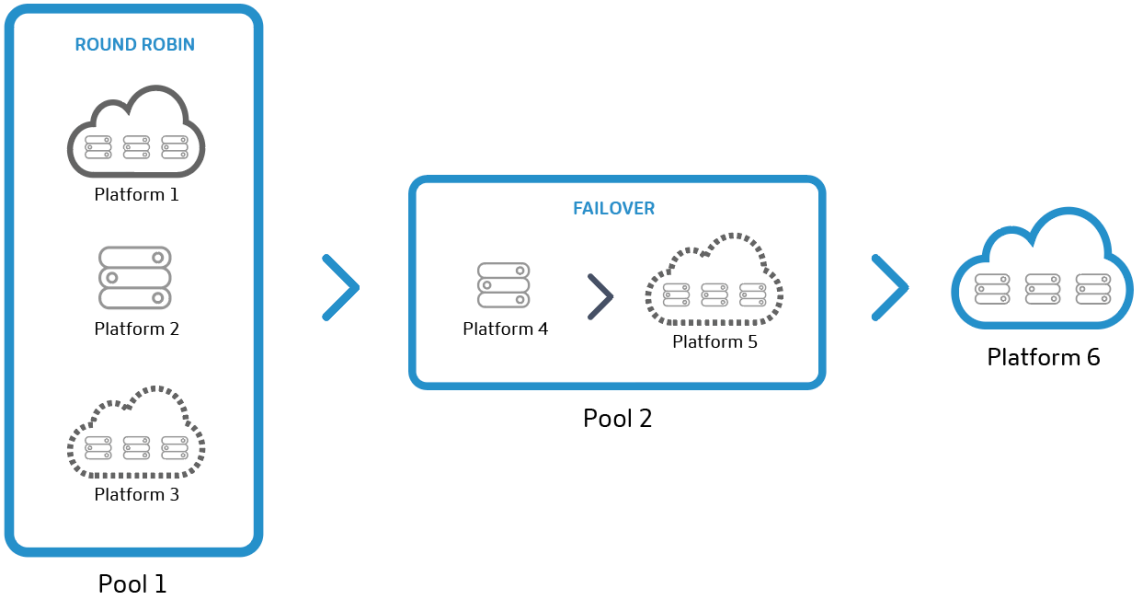
1. Haga clic en **Agregar una plataforma** en la parte superior derecha de esta sección.
2. Agregue todas las plataformas que desee que estén disponibles para el enrutamiento, incluidas las que deban agregarse a los grupos de direcciones. Para ello, haga clic en el campo **Elegir una plataforma** y seleccione plataformas individualmente en la lista.
3. Dependiendo del **tipo de respuesta** (A, AAAA o CNAME) seleccionado en la lista **Agregar registro**, escriba una dirección IPv4, una dirección IPv6 o CNAME para la plataforma. Puede volver a la sección **General** para modificar el **tipo de respuesta**, si es necesario.
4. Una vez seleccionada la plataforma y se introduce el **tipo de respuesta**, puede activar o desactivar la plataforma haciendo clic en el botón de alternancia **Habilitado**. También puede **activar/desactivar la disponibilidad del Radar y el Sonar** con botones de alternancia similares.
5. En la columna **Acciones**, elija el icono de marca de verificación para guardar los cambios o el icono de marca cruzada para cancelar.



Paso 2: Agregar y definir grupos de direcciones

Grupos de direcciones Los grupos de direcciones son una colección de plataformas que siguen un método de enrutamiento especificado por el usuario. El propósito de un grupo de direcciones es permitirle definir grupos lógicos de plataformas que se pueden utilizar con cualquier método de enrutamiento específico. Puede especificar métodos de enrutamiento **Round Robin** o **Conmutación por error** para que las plataformas sigan dentro de un grupo.

Puede agregar cualquier número de plataformas en cada grupo y cualquier número de grupos para cada una de sus ubicaciones geográficas. Por ejemplo, puede tener un grupo de la UE (formado por plataformas que dan servicio predominantemente a la región de la UE), un grupo de Asia (con plataformas en China, India y Singapur) y un grupo de Estados Unidos (con plataformas en Estados Unidos).

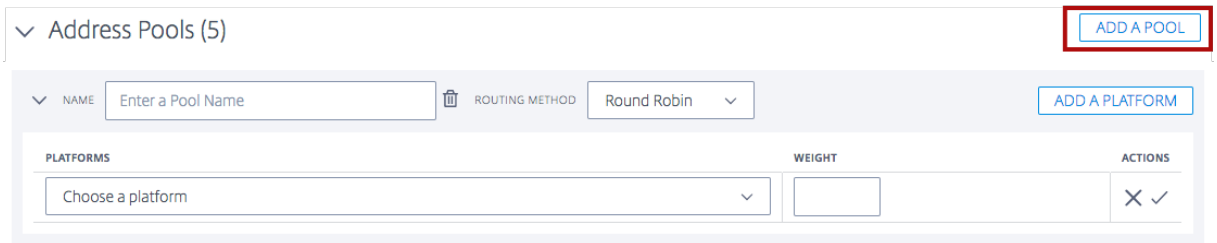


Nota: Los grupos de direcciones son opcionales. Puede tener plataformas individuales en su lugar y agregarlas a la configuración de enrutamiento.

Método de enrutamiento Round Robin Este tipo de enrutamiento sigue una metodología típica de equilibrio de carga de servidor global de round robin, donde cada CNAME/A/AAAA alterna se devuelve a los usuarios finales, a medida que se realizan solicitudes DNS. Por ejemplo, si las plataformas P1, P2 y P3 cumplen el umbral de disponibilidad, la primera solicitud se redirige a P1, la segunda a P2, la tercera a P3, la cuarta a P1 de nuevo, y así sucesivamente. También puede asignar pesos para la priorización y selección de cada plataforma a nivel mundial y/o por mercado o país.

Método de enrutamiento de conmutación por error Este método de enrutamiento admite una lógica de enrutamiento simple en la que se elige una plataforma en función de su lugar en la línea y su umbral de disponibilidad. Puede crear una cadena de conmutación por error que decida qué plataforma seleccionar primero, segundo, etc. Esta cadena de conmutación por error se puede crear para funcionar globalmente y/o para mercados y países individuales.

Adición de un grupo de direcciones Para agregar un grupo de direcciones, haga lo siguiente:



1. Haga clic en el botón **Agregar un grupo** en la parte superior derecha de la sección.
2. Introduzca un **nombre** para el grupo. El nombre se puede utilizar para identificar el propósito del grupo.
3. Seleccione un **método de enrutamiento**. Puede seleccionar **Round Robin** o **Conmutación por error**.
4. Elija una **plataforma** de la lista que creó en el paso anterior.
5. Puede agregar tantas plataformas a este grupo como sea necesario, haciendo clic en el botón **Agregar una plataforma**.
6. Para cada plataforma que elija, introduzca un **peso**adecuado. El propósito de los pesos es priorizar y seleccionar plataformas para la distribución del tráfico. Los pesos asignados a las plataformas no tienen que sumar hasta 100. Pueden ser cualquier entero entre 0 y 1 000 000. Estos pesos cuando se convierten en porcentaje (en el back-end), sumarán hasta un 100%. Si todas las plataformas seleccionadas reciben el mismo peso, el tráfico se distribuirá uniformemente entre ellas a lo largo del tiempo. Si solo tiene una plataforma, entonces esa se usará el 100% del tiempo, independientemente del peso que le dé.
7. Cuando termine, elija el icono de marca de verificación para guardar los cambios o el icono de marca cruzada para cancelar.
8. A continuación, puede modificar o eliminar la selección de la plataforma eligiendo los iconos apropiados en la columna **Acciones**.

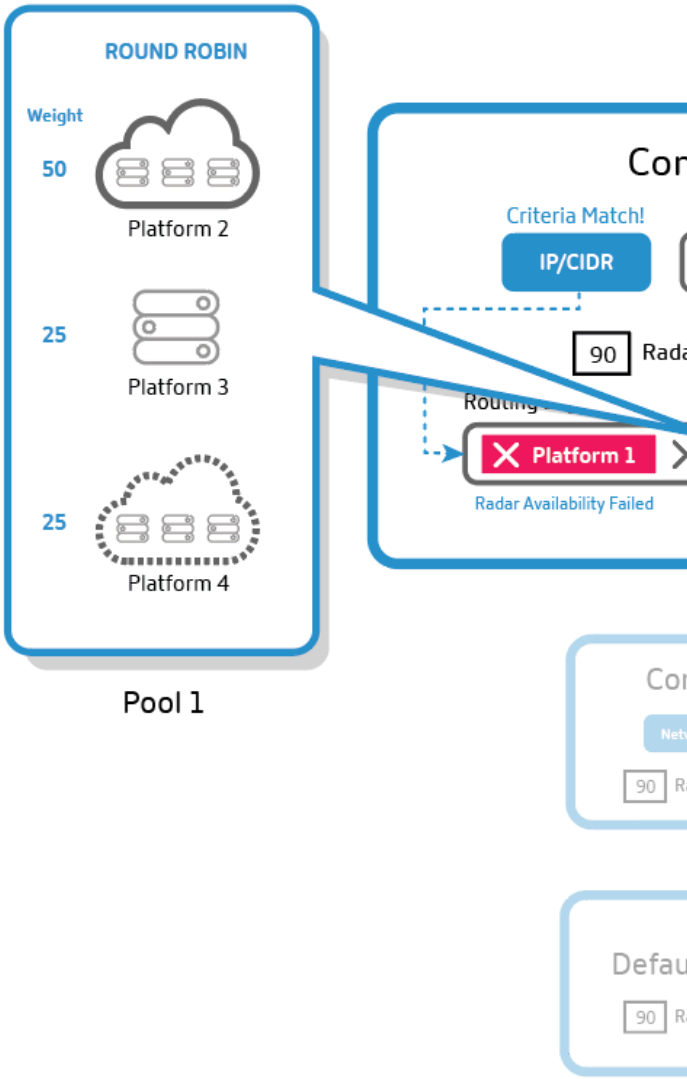
Paso 3: Configurar conmutación por error La conmutación por error se aplica a todo el conjunto de grupos de direcciones y/o plataformas individuales. Es compatible con un método de validación simple en el que se evalúa una plataforma o grupo individual para el enrutamiento en función de los siguientes criterios:

- Ubicación, red y/o IP/CIDR. Es necesario especificar al menos uno de estos criterios.

> **Nota:**
>
> Los criterios de ubicación para la conmutación por error no deben contener una combinación de continentes y países, pero puede utilizar la lógica de enrutamiento para crear

> varias conmutaciones por error.

- Disponibilidad de Sonar y Radar si está configurado
- Lugar en la cola



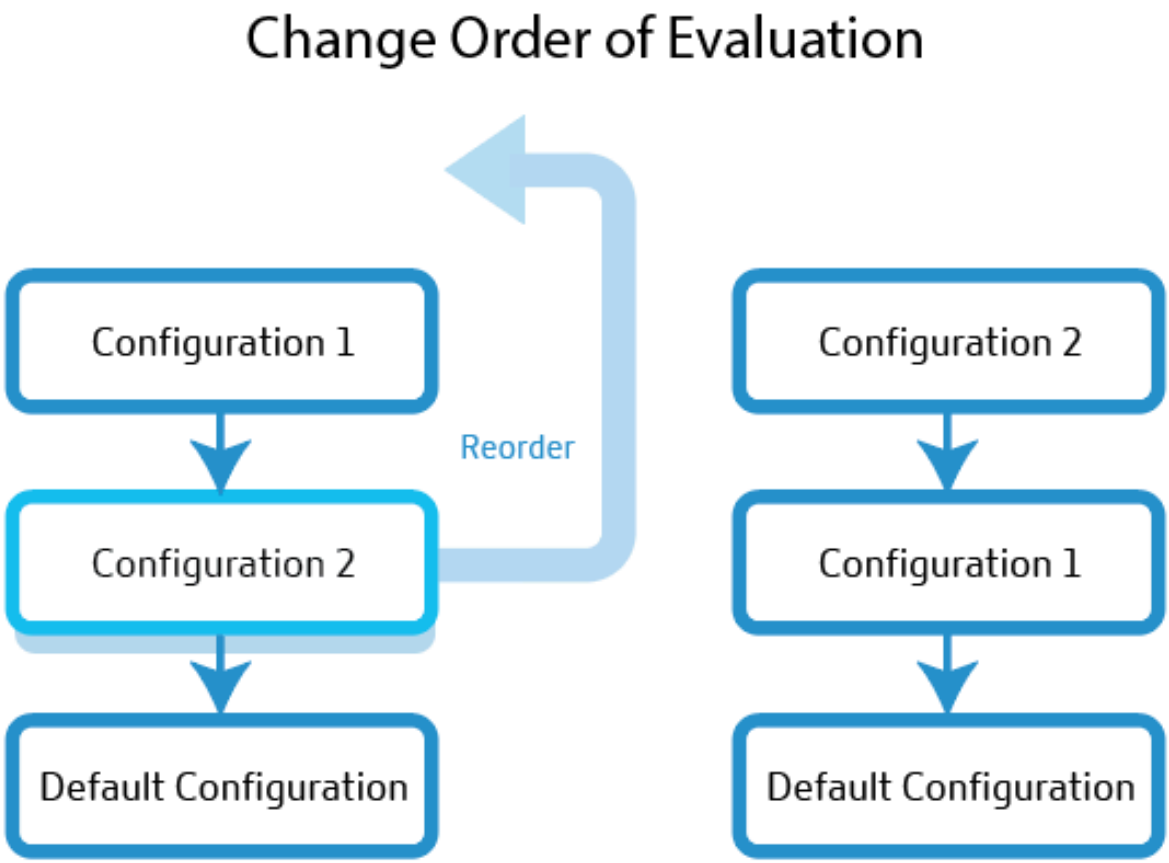
Conmutación por error para registros predictivos

1. El registro predictivo evalúa el primer bloque de configuración para los criterios requeridos (ubicación, red y/o IP). Si el primer bloque de configuración de ruteo no cumple los criterios requeridos, pasa al segundo en línea y así sucesivamente.
2. El bloque de configuración que cumple con todos los criterios requeridos, se elige para la distribución del tráfico.
3. Dentro del bloque de configuración elegido, los grupos de direcciones o plataformas se evalúan en función de su lugar en línea y el umbral de disponibilidad (Radar y Sonar).

4. La primera plataforma dentro del grupo de direcciones (o fuera de él) que cumple el umbral de disponibilidad, se selecciona para la distribución del tráfico. Luego entra en juego la lógica de enrutamiento Round Robin o Conmutación por error.

Nota: Si solo hay una plataforma en el grupo, esa plataforma se selecciona 100% del tiempo, y la lógica de round robin no se aplicará a ella.

Como usuario, puede organizar los bloques de configuración de enrutamiento de tal manera que el que tiene la prioridad más alta sea primero en línea y así sucesivamente. El reordenamiento se puede hacer manualmente arrastrando cada grupo o plataforma a donde debe estar en la línea.



Configuración predeterminada Debe tener al menos una plataforma o grupo en el bloque de configuración de enrutamiento predeterminado. Debe contener una o más plataformas o grupos que utilizará el registro Predictive si todas las demás opciones no coinciden con los criterios especificados. El valor predeterminado no tiene ningún criterio para especificar y coincide con todas las solicitudes. Si la disponibilidad de la plataforma no cumple el umbral de disponibilidad del Radar, la respuesta devuelve la reserva.

Pasos para configurar la conmutación por error Para definir la configuración, haga lo siguiente:

1. Introduzca un **nombre**. Este nombre ayuda a identificar el bloque de configuración de enrutamiento.
2. Puede dejar el TTL predeterminado tal cual, o modificarlo según sus necesidades.
3. Asegúrese de que la **disponibilidad del Radar** está marcada. Puede establecer el umbral de disponibilidad del Radar al nivel deseado. Al desactivar esta opción, se inhabilita Radar para el conjunto de grupos o plataformas.
4. Seleccione **Ubicaciones, Redes y/o IP/CIDR**. Por ejemplo, si la configuración de enrutamiento se aplica a la región Oceanía, puede especificar ubicaciones, redes y direcciones IP /o de plataformas o grupos de esta región.
5. El campo **Configuración de conmutación por error** le permite establecer la prioridad de selección para todos los grupos y plataformas. El orden en el que coloque estos grupos o plataformas determinará su selección para el enrutamiento. Y el tráfico se enrutará según el método especificado (round robin o failover) en el paso anterior.
6. Para eliminar un bloque de configuración, haga clic en el icono de papelera situado junto al campo **Nombre**.

Informes DNS

Los informes DNS proporcionan una potente visibilidad del volumen de solicitudes DNS en función de varios criterios para un dominio o nombre de host especificado. Muestran la frecuencia con la que se consultan tipos de registros específicos y proporcionan un nivel completamente diferente de detalle. Este grado de granularidad permite a los usuarios de DNS predictivo comprender tendencias y volúmenes de consulta para zonas específicas, nombres de host, tipos de solicitud, mercados, países, regiones, estados y redes.

Estos informes se utilizan principalmente para una mejor visibilidad y análisis. Dan flujos de tráfico para cada zona o nombre de host y ayudan a diagnosticar problemas relacionados con DNS. También revelan anomalías como picos en las solicitudes u otras irregularidades, desglosando el volumen de solicitudes por tipos de registro y ubicaciones.

También puede filtrar el ruido innecesario sabiendo qué zonas sirven más tráfico y centrarse únicamente en las zonas o tipos de registro que le interesan.

DNS frente a Informes de Openmix

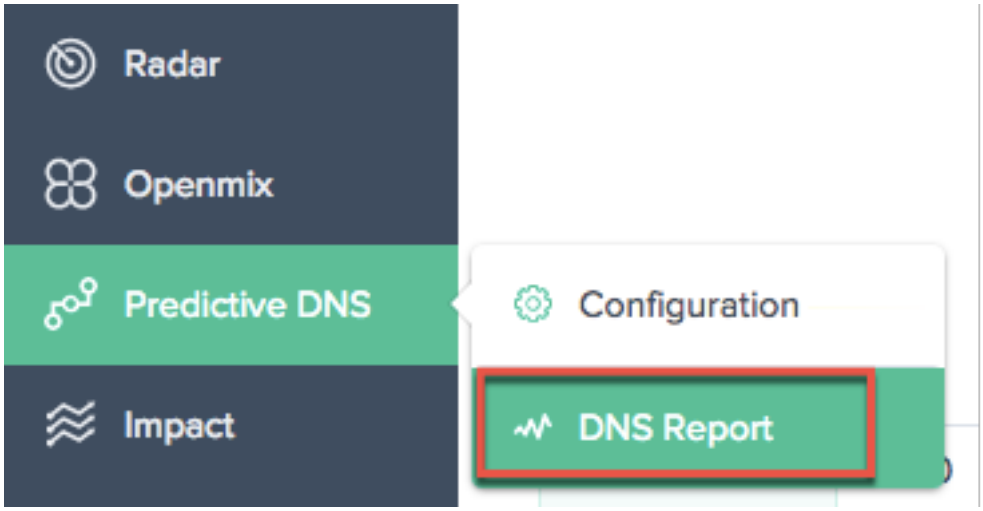
Para los clientes de Openmix, los informes aparecen dentro de los informes DNS y en los informes de decisión de Openmix. Los informes DNS proporcionan información sobre las solicitudes realizadas

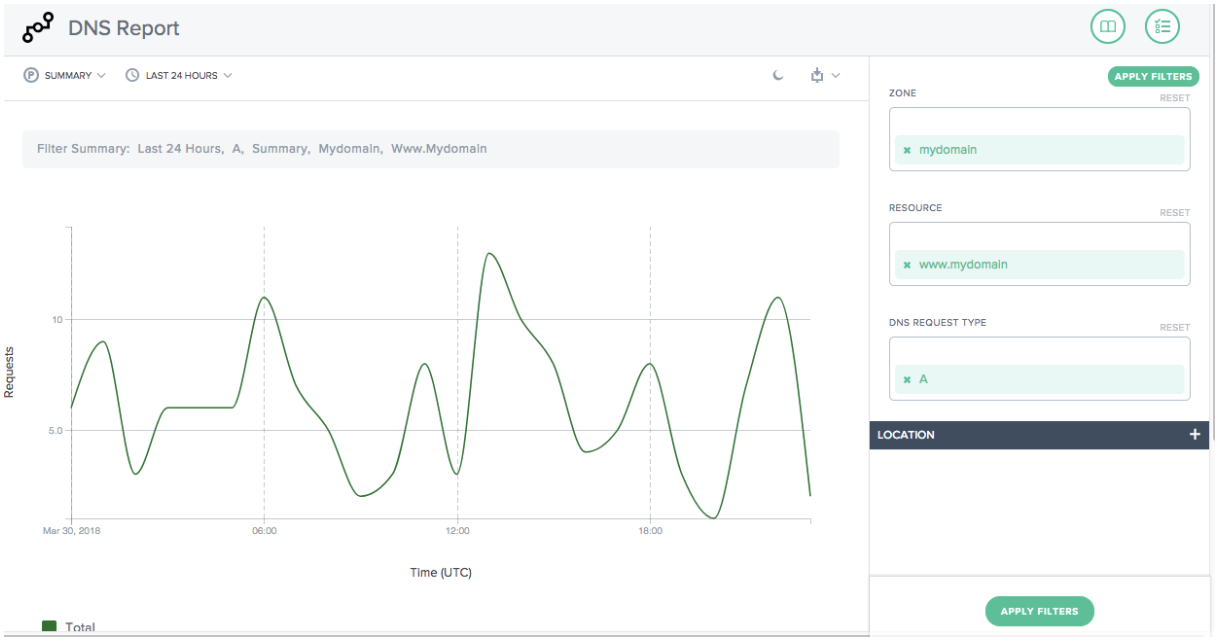
a nuestras zonas autorizadas, mientras que Openmix proporciona informes sobre cuándo se utilizó la plataforma inteligente Openmix para satisfacer una solicitud, ya sea a través de un registro de aplicación Openmix o directamente a un CNAME Openmix.

Navegación

Para ir a la sección **Informe DNS**:

1. Haga clic en **DNS predictivo** en el menú de navegación izquierdo.
2. Desplácese hasta **Informe DNS**.
3. Se abrirá la página **Informe DNS**.

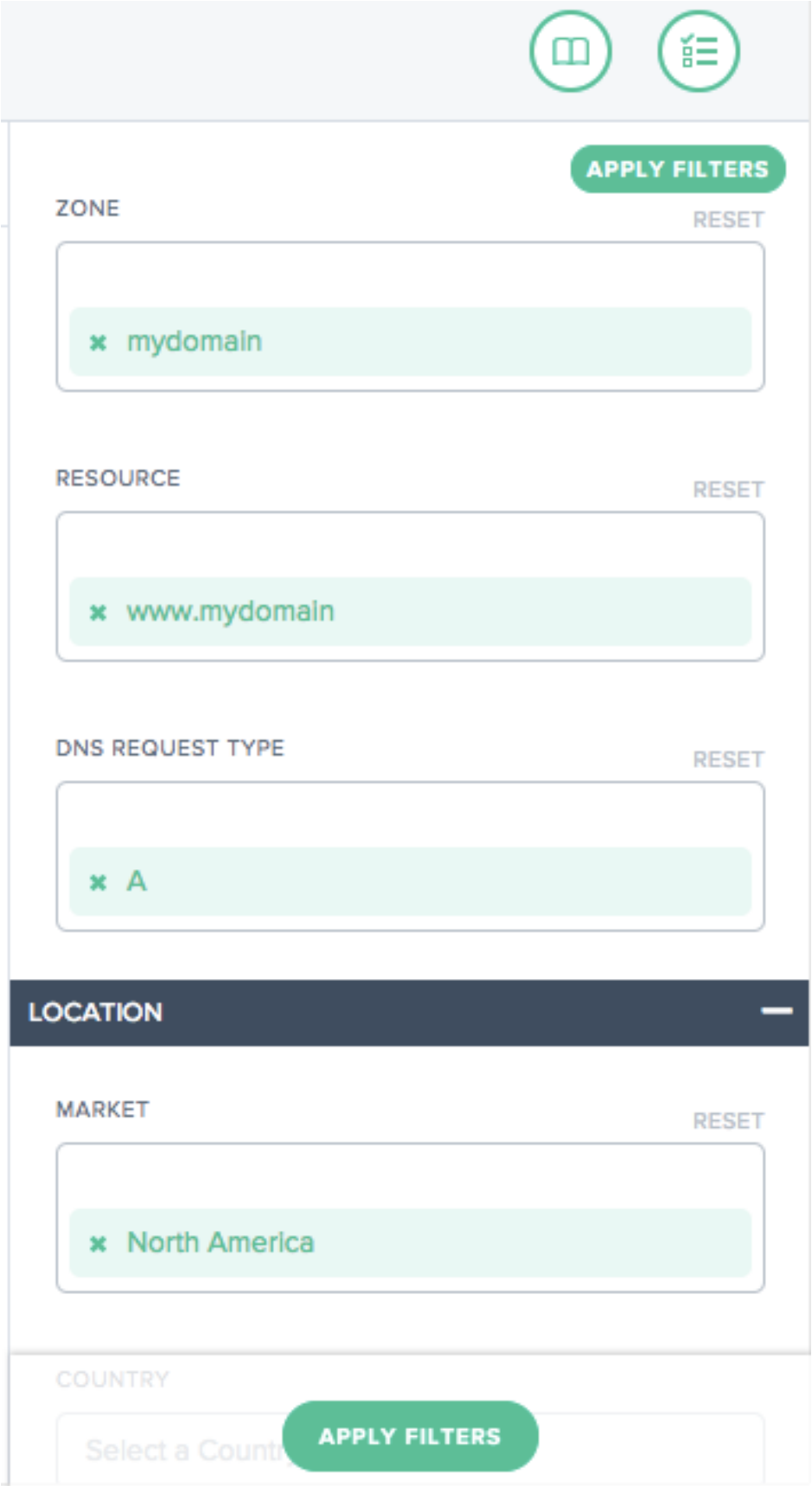




Aplicar filtros

El panel **Aplicar filtros** de la derecha le ayuda a seleccionar y ver solo los datos que desea mostrar en el informe.
Puede filtrar según lo siguiente:

- **Zona**: Seleccione una o más zonas para incluir.
- **Recurso**: Seleccione uno o varios nombres de host que desee incluir.
- **Tipo de solicitud DNS**: Seleccione uno o varios tipos de solicitud DNS que desea incluir.
- **Ubicación**: Seleccione una o varias ubicaciones geográficas (Mercado, Región, Estado o Red) que desea incluir.



Dimensión principal

Las dimensiones principales se seleccionan a través de listas sobre el gráfico. Puede usar esto como un potente pivote en el informe.

Resumen El resumen proporciona el número total de solicitudes con el conjunto completo de los filtros aplicados.

Filtrar por intervalos de tiempo predefinidos

Los intervalos de tiempo preestablecidos relativos se pueden elegir como filtro adicional para refinar aún más los informes.

Informes de marcadores

Una vez que genere un informe basado en los criterios de filtro, puede guardar los filtros aplicados marcando el informe. Cada vez que visita este marcador, se genera un informe actualizado basado en todos los filtros seleccionados.
Para marcar un informe, haga lo siguiente:

- Haga clic en el icono de marcador situado en la parte superior derecha de la página.
- En el cuadro de diálogo Agregar nuevo marcador, asigne un nombre apropiado al marcador y haga clic en Crear.
- Ahora se crea un nuevo marcador. Puede acceder al marcador haciendo clic en el icono de marcador (en la esquina superior derecha de cada página del informe) y seleccionando el marcador.

Sonar

June 4, 2021

Sonar es un servicio de comprobación de capacidad que se puede utilizar para supervisar la disponibilidad de servicios basados en la web. Sonar funciona realizando solicitudes HTTP o HTTPS desde múltiples puntos de presencia alrededor del mundo a una URL que especifique.

Conceptos básicos de Sonar

Los dispositivos de punto final probados por Sonar se consideran arriba o abajo en función de los siguientes criterios:

- Las solicitudes que dan como resultado HTTP 2xx se consideran exitosas y cualquier otro resultado, incluidos los problemas de red y los tiempos de espera, se tratan como errores.
- Sonar sigue las respuestas de redirección que devuelven códigos de estado 3xx, para un máximo de 6 redirecciones, hasta que recibe respuesta no 3xx o se produce un error.
- El estado del punto final se decide en función del quórum de las ubicaciones de informes. Sonar informa cualquier resultado (éxito o fracaso) que devuelve la mayoría de los puntos de presencia.

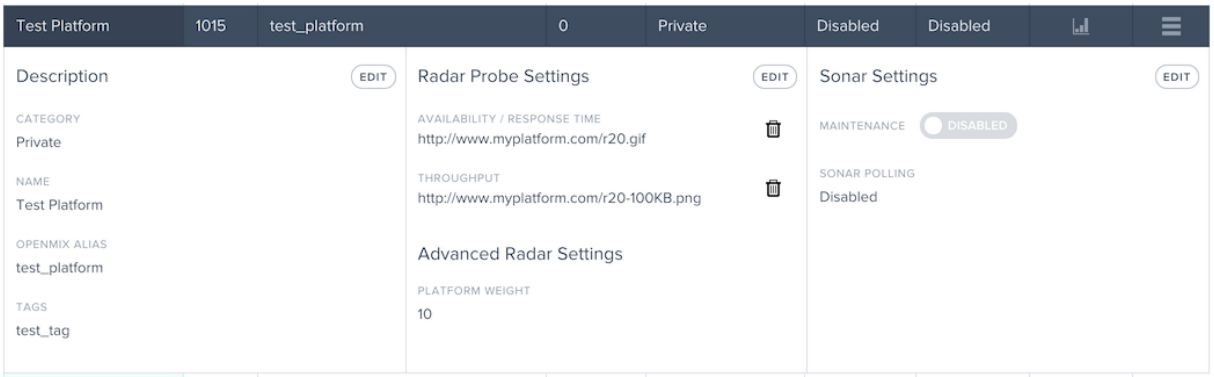
Las comprobaciones de Sonar se realizan desde múltiples ubicaciones de pruebas de todo el mundo. Las ubicaciones incluyen:

- Singapur
- Carolina del Sur, Estados Unidos
- Tokio, Japón
- St Ghislain, Bélgica
- Washington, Estados Unidos
- New York, Estados Unidos
- Londres, Inglaterra
- Hong Kong
- Frankfurt, Alemania
- Dublín, Irlanda
- Iowa, Estados Unidos de América
- Virginia, Estados Unidos
- Ámsterdam, Países Bajos

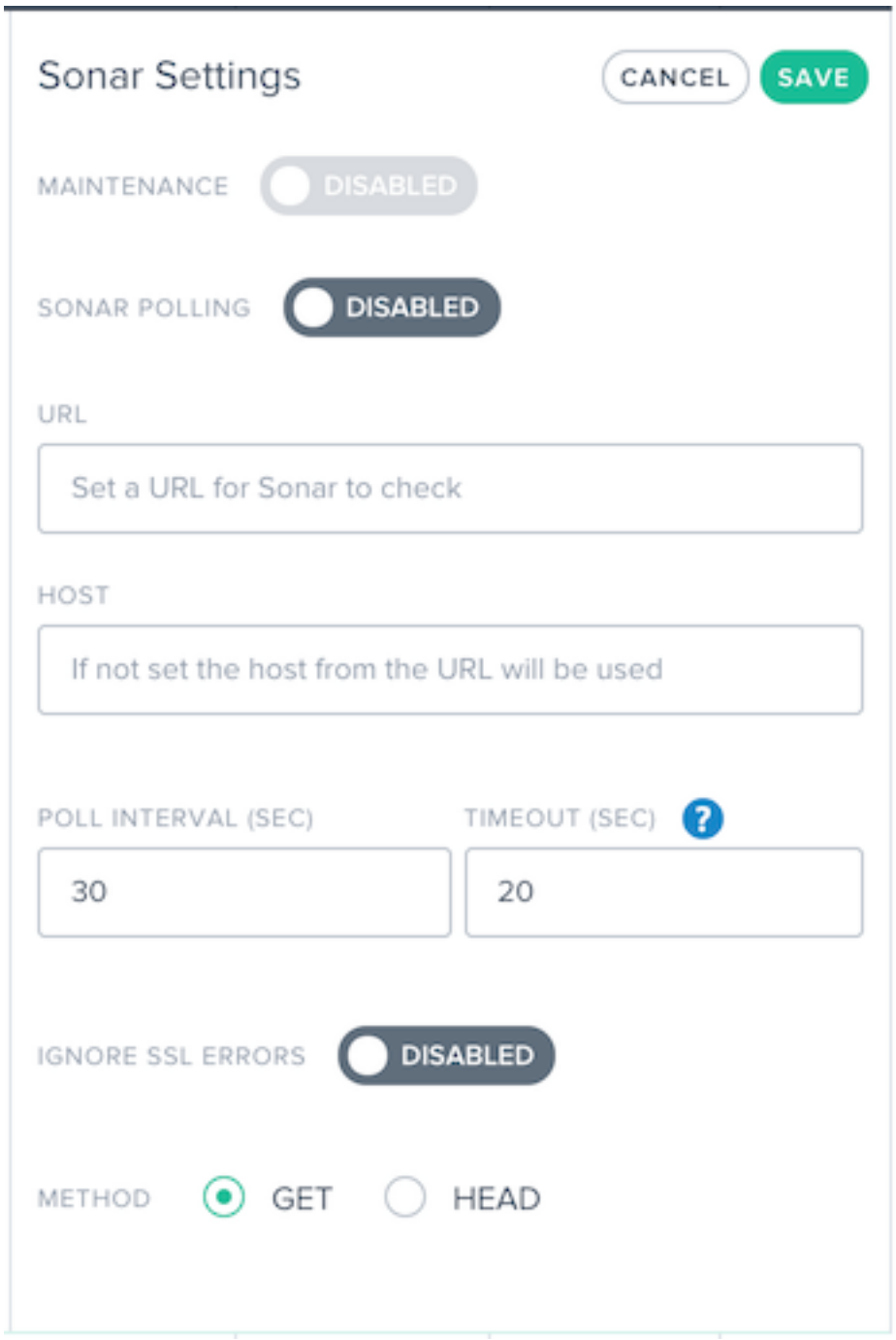
La plataforma Sonar está estrechamente integrada con los servicios globales de la plataforma Radar, Fusion y Openmix. Los datos de Sonar se alimentan en tiempo real a todos los nodos Openmix alrededor del mundo, para ser utilizados como una entrada adicional para la toma de decisiones.

Configuración de Sonar de Plataforma

Sonar está configurado para cada plataforma de la página Plataformas. Haga clic en una plataforma de la lista para ver la sección **Configuración de Sonar**.



Para agregar la supervisión de Sonar a la plataforma, haga clic en el botón **Modificar** en la sección **Configuración de Sonar**.

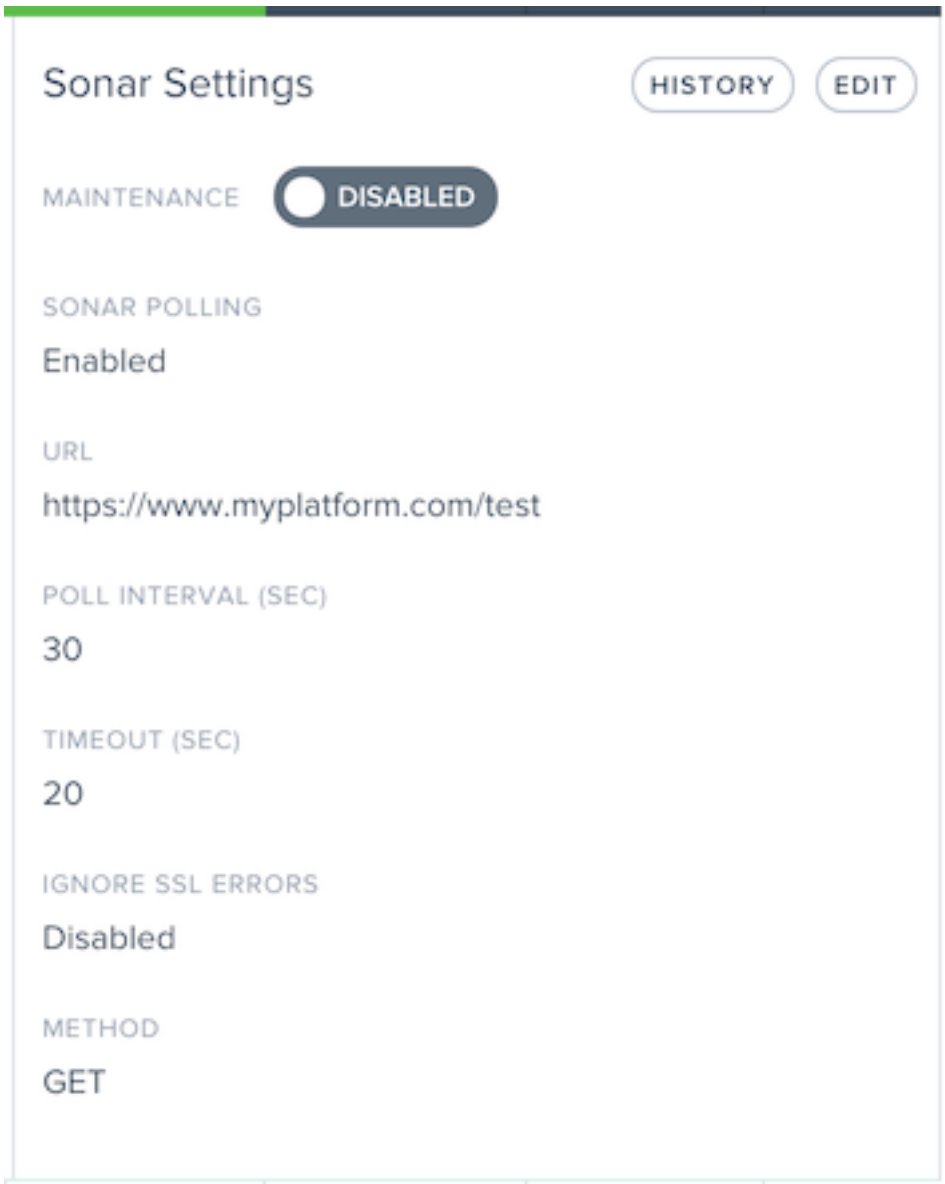


A continuación se describen los campos:

Elemento de entrada	Descripción	Predeterminado
Mantenimiento	Cuando está habilitado, Sonar informará que el servicio está inactivo independientemente del estado real. Esto es útil cuando se desea eliminar una plataforma del enrutamiento Openmix en previsión del tiempo de inactividad.	Inhabilitada
Sondeo de sondeo	Si está habilitado, Sonar realizará comprobaciones en la URL configurada.	Inhabilitada
dirección URL	La URL Sonar llama para comprobar la disponibilidad del servicio.	
Host	El valor que se debe utilizar para el valor de encabezado Host en la solicitud.	v
Intervalo encuesta	Frecuencia especificada en segundos para comprobar la disponibilidad del servicio. Las comprobaciones pueden tener un intervalo mínimo de cada segundo hasta 300 segundos (5 minutos).	60 v
Tiempo de espera	Cantidad de tiempo especificada en segundos para esperar una respuesta antes de asumir una comprobación fallida en el servicio. Las comprobaciones pueden tener un tiempo de espera mínimo de 1 segundo hasta 30 segundos. Para intervalos de sondeo más bajos, por ejemplo, por debajo de 5 segundos, el tiempo de espera se limitará a 4 segundos.	20

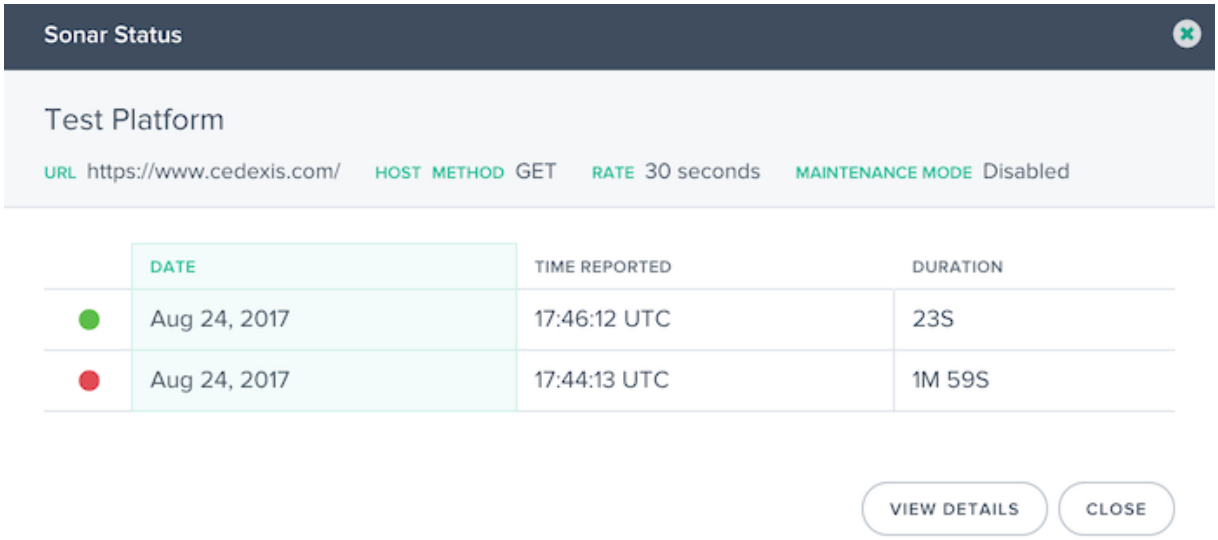
Elemento de entrada	Descripción	Predeterminado
Ignorar errores SSL	Cuando se habilita, Sonar ignorará los errores SSL que se produzcan durante la solicitud, como un certificado SSL mal configurado.	Inhabilitada
Método	El método HTTP utilizado para la comprobación: GET o HEAD.	

Para activar Sonar, cambie **Sondeo de Sonar** a **Habilitado** e introduzca la URL del servicio. Haga clic en **Guardar** y se iniciarán las comprobaciones.



Cuando Sonar está habilitado, la configuración muestra la configuración actual de Sonar.

Una vez habilitado el Sonar, puede hacer clic en el botón **Historial** en la sección **Configuración de Sonar** para ver los cambios de estado recientes y la duración. Haga clic en el botón **Ver detalles** para ir a la página Estado de la plataforma Sonar para obtener más detalles e informes de estado a largo plazo.



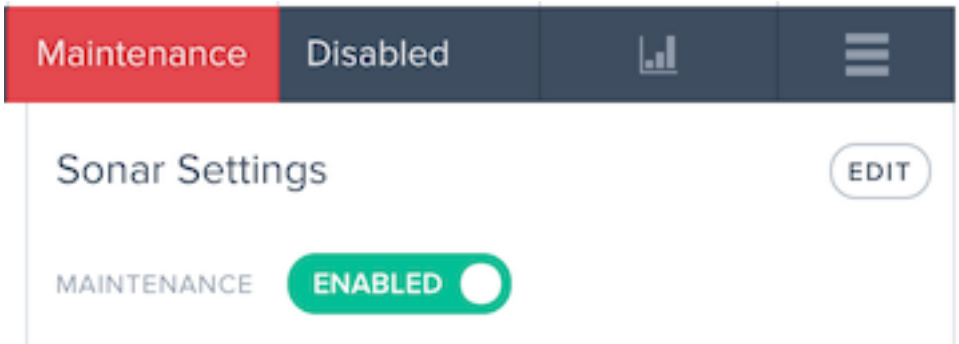
Estado de Sonar de plataforma

Cuando Sonar está habilitado para una plataforma, el estado de Sonar se muestra en la lista de plataformas en la columna **Sonar**. Cuando la supervisión de Sonar se compara con la plataforma, la celda de columna es verde y muestra la cantidad de tiempo que la plataforma ha sido alcanzada.

Si las comprobaciones de supervisión de la plataforma han fallado, la celda **Sonar** es roja y mostrará la cantidad de tiempo que la plataforma ha sido inalcanzable.

Modo de mantenimiento

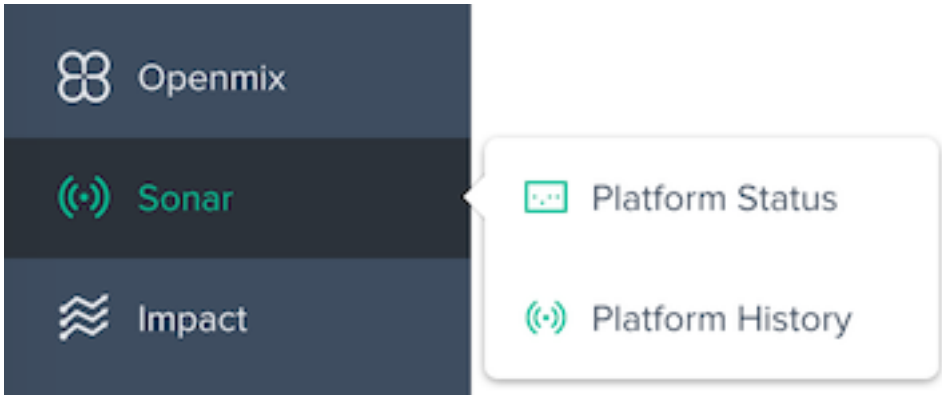
El estado de Sonar muestra la disponibilidad del servicio en función del éxito o el fracaso de las comprobaciones sintéticas. Si desea marcar la plataforma como inactiva aunque sea accesible, **por** ejemplo, en previsión del mantenimiento en la plataforma, puede activar el modo de mantenimiento. Este modo informa de que la plataforma no está disponible en las aplicaciones Openmix y detendrá automáticamente el tráfico que se entregue a la plataforma en cualquier aplicación Openmix que tenga Sonar habilitado.



Activar Modo de mantenimiento, cambie la opción **Mantenimiento** a **Habilitado**.

Una vez habilitado, el elemento de lista de plataformas muestra el estado de Sonar como **Mantenimiento**.

Menú Sonar



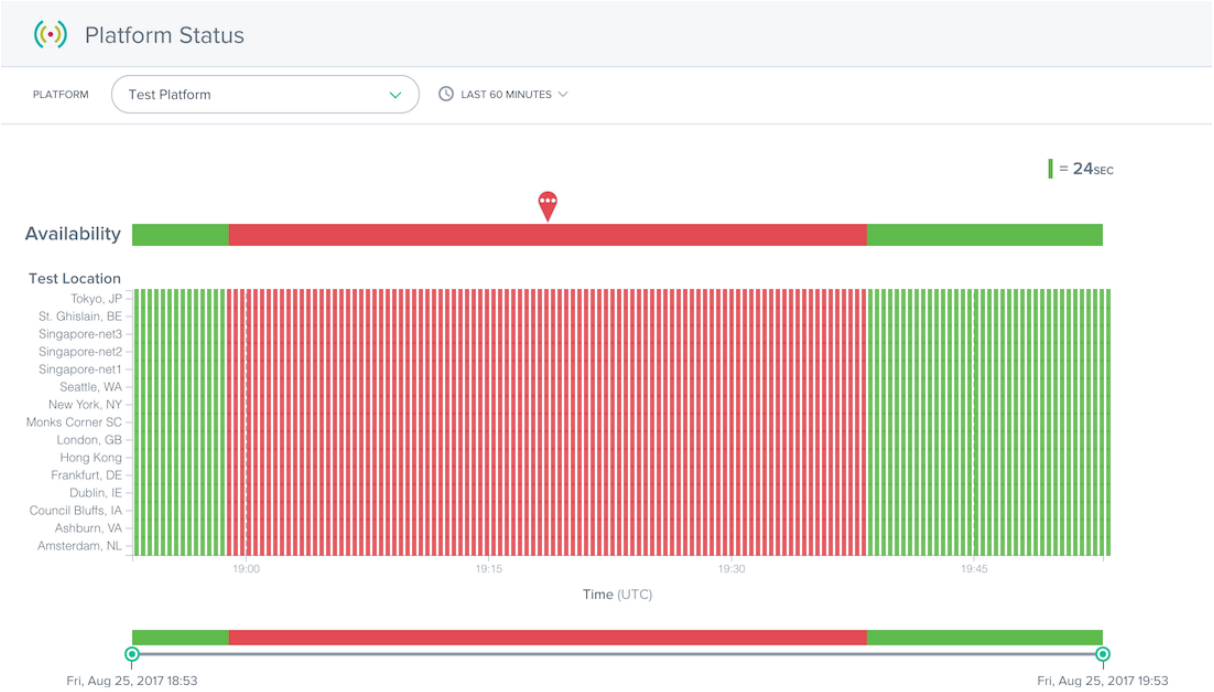
El menú **Sonar** se compone de las siguientes opciones:

1. **Estado de la plataforma**: Resultados detallados por ubicación de prueba y el estado general de disponibilidad.
2. **Historial de plataformas**: Descripción general del estado de disponibilidad en los últimos tres meses.

Estado de la plataforma

El informe Estado de la plataforma Sonar muestra detalles de las comprobaciones realizadas por cada ubicación de prueba y el estado general calculado a partir de los datos agregados.

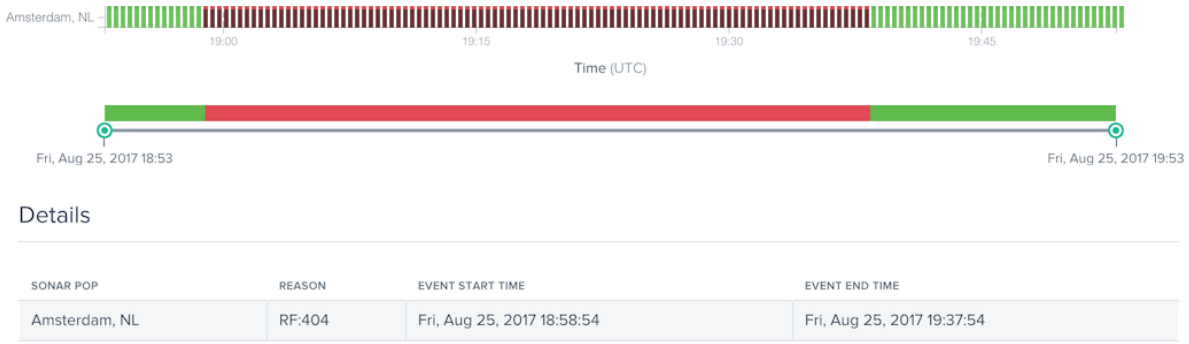
Para obtener información sobre una plataforma específica, seleccione una plataforma en el menú **Plataformas**.



El informe de estado contiene las siguientes secciones:

- Disponibilidad: En la parte superior del informe se encuentra la disponibilidad reportada a Openmix en función de los resultados agregados de las ubicaciones de prueba individuales. Este es el estado de Sonar que se utilizó en las aplicaciones Openmix durante los tiempos especificados.
- Ubicaciones de prueba: Se muestran los resultados de cada ubicación de prueba.
- Control deslizante de tiempo: el control deslizante de tiempo le permite perforar fácilmente en períodos de tiempo detallados. Arrastre los controles deslizantes de tiempo para ajustar el período de tiempo del informe y ver intervalos de tiempo más detallados.

Los detalles de las comprobaciones fallidas se pueden ver haciendo clic en un marcador rojo en una fila de ubicación de prueba. Los detalles de las fallas de prueba se mostrarán en la sección **Detalles** debajo del informe.



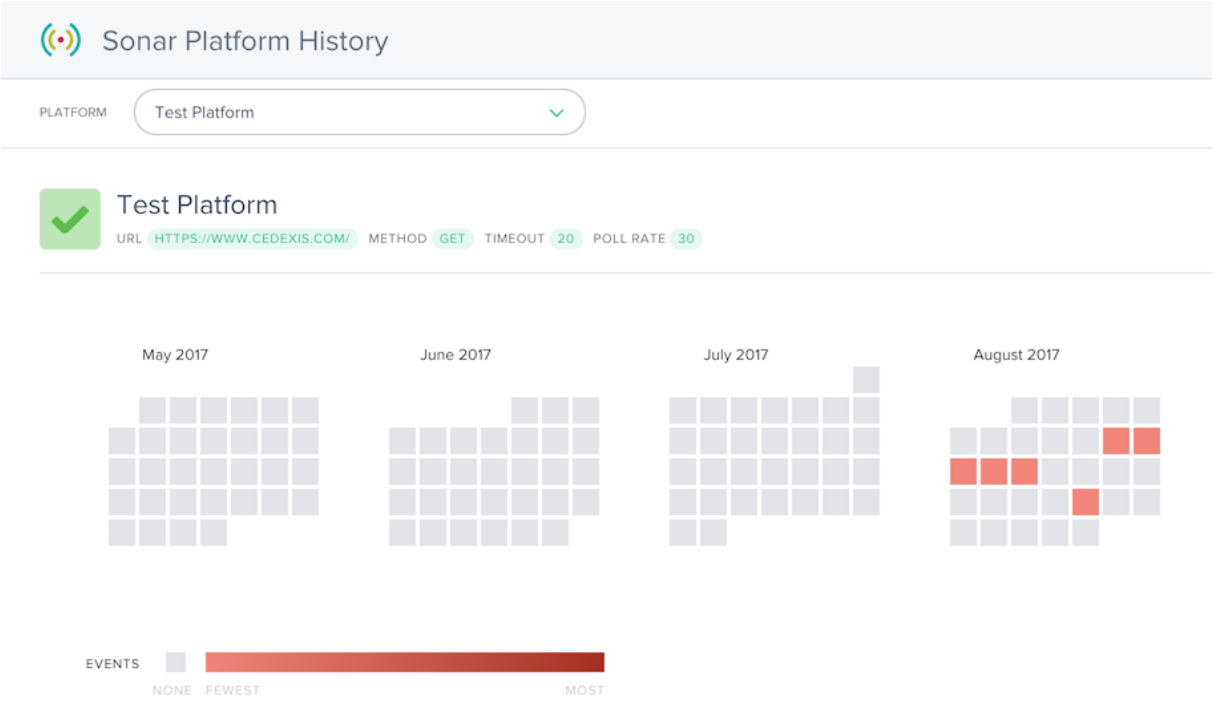
La columna **Motivo** proporciona detalles como el código de error devuelto por las comprobaciones

de Sonar que se produjeron en esa ubicación de prueba.

Historial de plataformas

El informe Historial de la plataforma Sonar muestra el estado de disponibilidad de las comprobaciones agregadas realizadas por cada ubicación de prueba en los últimos meses.

Para obtener información sobre una plataforma específica, seleccione una plataforma en el menú **Plataformas**.



El informe Historial muestra un calendario de los últimos meses. Los días que tienen interrupciones de servicio se muestran en gradientes de color rojo. Cuantos más eventos de disponibilidad ocurran el día, más rojo se mostrará.

Debajo del calendario hay una lista de cortes de servicio que se han producido y algunos detalles básicos sobre los eventos.

Details

DATE	OUTAGES	START TIME - FIRST OUTAGE	END TIME - LAST OUTAGE	DURATION
2017-08-11	1	21:29:35	23:59:59	2 hours, 30 minutes, 25 seconds
2017-08-12	1	00:00:00	23:59:59	24 hours, 0 minutes, 0 seconds
2017-08-13	1	00:00:00	23:59:59	24 hours, 0 minutes, 0 seconds
2017-08-14	1	00:00:00	21:21:18	2 days, 23 hours, 51 minutes, 43 seconds
2017-08-15	3	14:50:00	15:50:05	0 hours, 4 minutes, 3 seconds
2017-08-24	3	17:44:12	18:03:21	0 hours, 15 minutes, 25 seconds

Puede hacer clic en el día natural o en la fecha en las columnas **Detalles** para cargar el informe Estado para obtener más detalles sobre la interrupción del servicio.

Impact

April 24, 2020

Impact ofrece una visión eficaz del rendimiento y de los datos de KPI empresariales recopilados mientras los visitantes están en su sitio. Haga clic en el enlace para ver los datos de informes que le interesan para ver más detalles.

Informes de visualización de plataformas en la nube

El menú **Impact** se compone de las siguientes opciones:

1. Datos de sincronización de navegación : Detalles de rendimiento a nivel de página, también conocidos como nuestros informes de tiempo de carga de página.
2. Datos de repetición de vídeos : Calidad de la experiencia y datos de entrega de vídeo.
3. Datos de temporización de recursos : Detalles de rendimiento de recursos individuales en páginas.

Datos de sincronización de navegación

September 13, 2023

Los informes de sincronización de navegación ofrecen una visión eficaz de la carga de páginas enriquecidas y los datos de rendimiento de eventos recopilados mientras los visitantes están en su sitio.

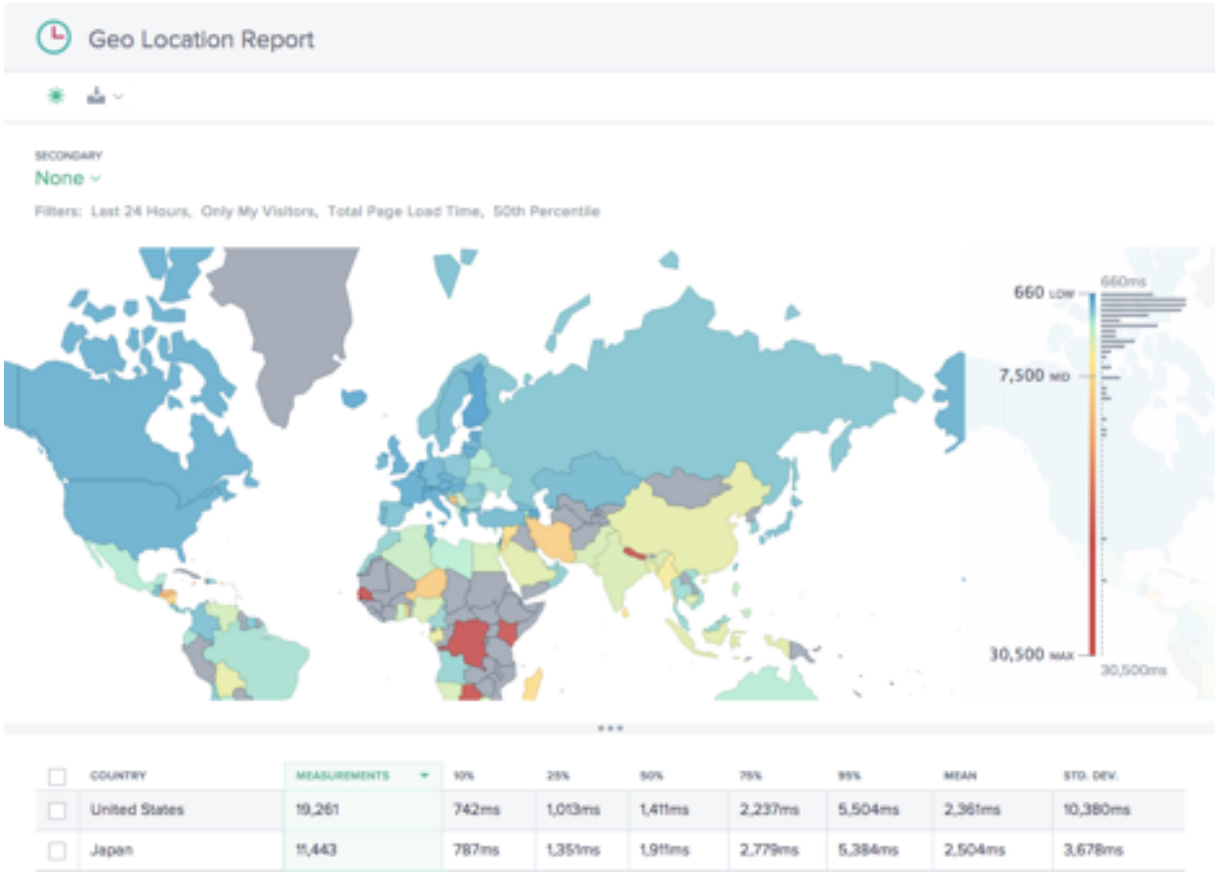
Después de una breve descripción de los informes, hay detalles sobre cómo pivotar, filtrar y personalizar los informes de sincronización de navegación.

Informes de temporización de navegación

El menú **Temporización de navegación** incluye los siguientes informes:

1. Informe de**ubicación geográfica: informe** de temporización de navegación por dimensión geográfica.
2. **Informe de rendimiento** : datos de medición del tiempo de navegación a lo largo del tiempo.
3. **Informe de distribución estadística** : vista de los datos de temporización de navegación a través de una vista de informes de distribución estadística.

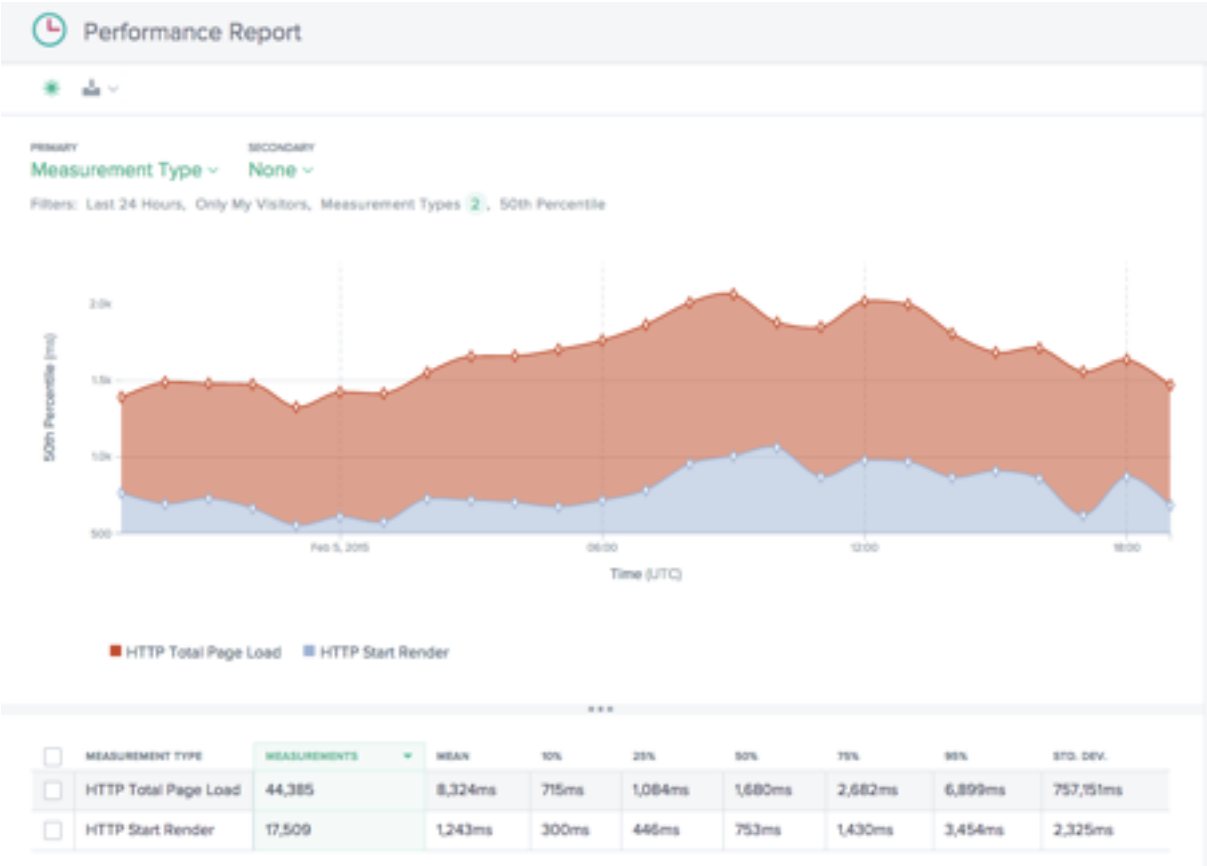
Informe de ubicación geográfica



Este informe muestra el rendimiento del tiempo de carga de página para cada país. Amplíe el mapa para ver una mayor granularidad según sea necesario.

La tabla muestra cada país con su rendimiento de tiempo de carga de página asociado, junto con el número de mediciones (vistas de página).

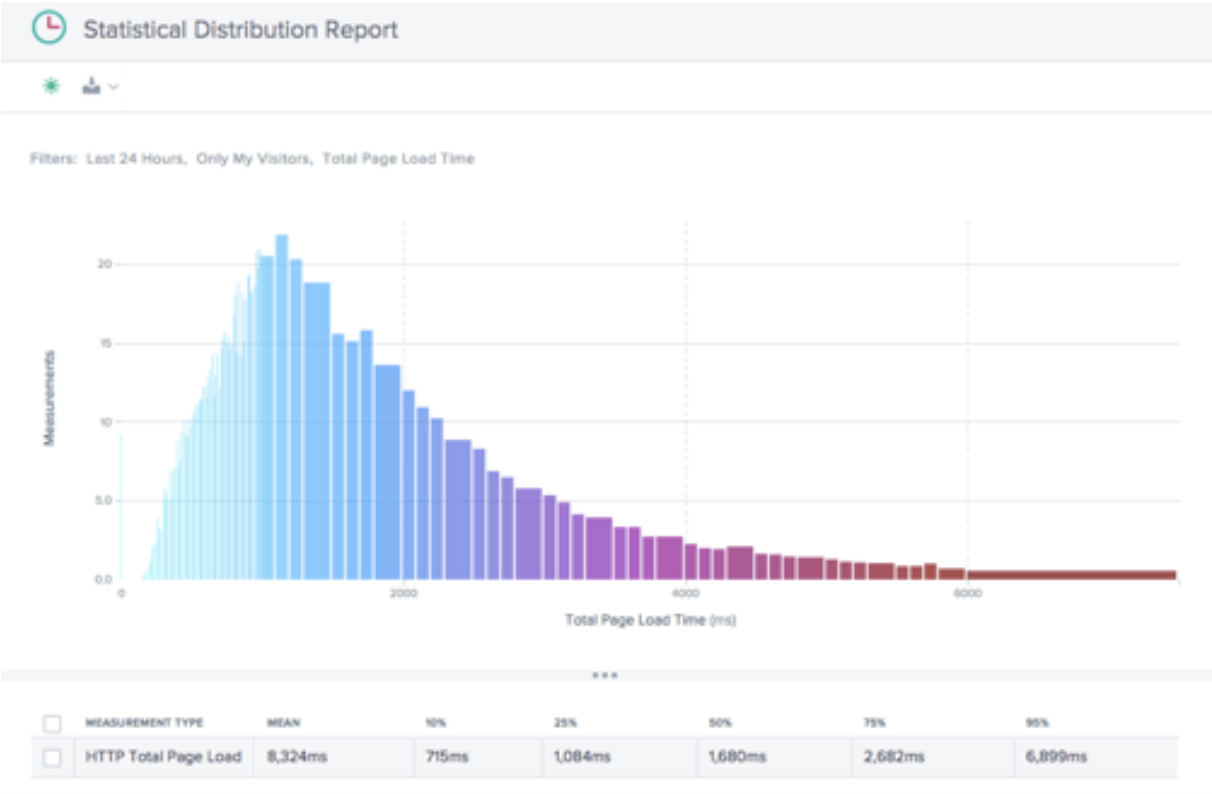
Informe de rendimiento



Este informe muestra el rendimiento del KPI de sincronización de navegación a lo largo del tiempo desglosado por tipo de medida.

De forma predeterminada, se seleccionan Iniciar modelizado y Tiempo total de carga de página. Se pueden agregar otros tipos de medida según sea necesario.

Informe de distribución estadística



Este informe muestra la distribución estadística de los valores de tiempo de navegación y tiempo de carga de página.

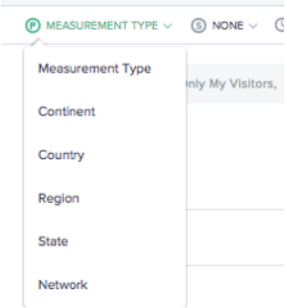
El informe proporciona información sobre cuántas mediciones (Vistas de página) se recogieron por valor de tiempo de carga de página.

Uso de informes de temporización de navegación

Para refinar y personalizar las vistas de informes para necesidades específicas de informes, utilice la siguiente funcionalidad en los informes Temporización de exploración.

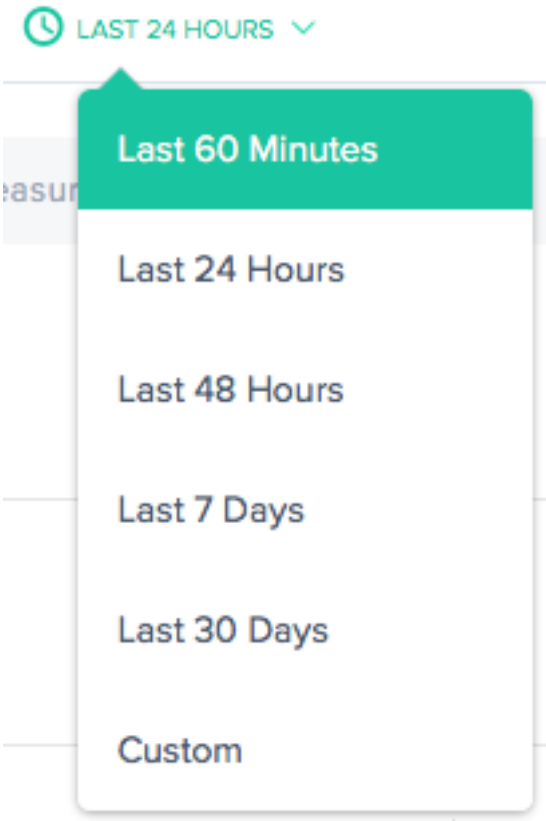
Además de las funciones estándar de los informes, como compartir informes, alternar en segundo plano, exportar datos y más, están disponibles las siguientes funciones:

Cotas primaria y secundaria



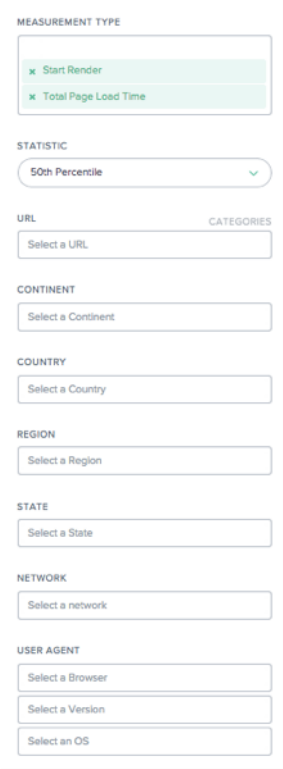
La dimensión principal del gráfico se selecciona mediante una lista de selección situada encima del gráfico. Utilícelo como un potente pivote en el informe para expresar los datos en términos de tipo de medida (predeterminado), continente, país, región, estado o red (ASN). También se puede elegir una dimensión secundaria para refinar aún más los informes.

Filtro: Rango de tiempo del informe



Los informes se pueden generar con un intervalo de tiempo de últimos 60 minutos, últimas 24 horas, últimas 48 horas, últimos 7 días, últimos 30 días o un rango personalizado. La vista predeterminada es las últimas 24 horas.

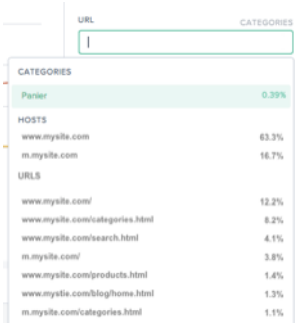
Filtros: Potentes capacidades de profundización



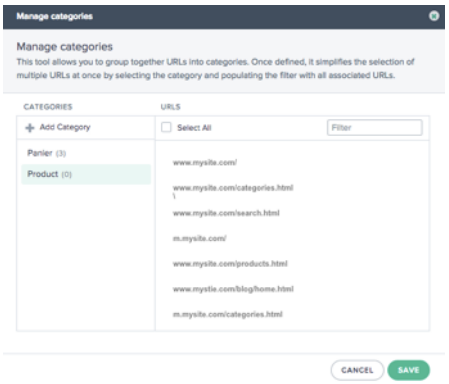
Los informes varían ligeramente en términos de qué filtros son apropiados en función de los datos. Los siguientes informes están disponibles en los informes de sincronización de navegación:

- **Tipo de medida**: Seleccione uno o varios tipos de medida para ver. El procesamiento inicial y el tiempo total de carga de página están seleccionados de forma predeterminada.
- **Estadística**: Seleccione una medida estadística para ver los datos.
- **URL**: Seleccione una o más URL para ver. Además, puede seleccionar un nombre de host o una categoría de URL (ver más abajo).
- **Continente**: Seleccione uno o más continentes para incluir
- **País**: Seleccione uno o más países para incluir
- **Región**: Seleccione una o más regiones geográficas (cuando corresponda) para incluir
- **Estado**: Seleccione uno o más estados geográficos (cuando corresponda) para incluir
- **Red**: Seleccione una o más redes (ASN) para incluir
- **Agente de usuario**: Seleccione uno o más exploradores, versión del explorador y/o sistema operativo para refinar aún más los datos de informes.

Categorías de URL



Los informes de sincronización de navegación se pueden filtrar por URL, Hosts o Categorías. Encuentre rápidamente uno o más elementos de interés escribiendo en el cuadro de **búsqueda de URL**.



Para crear una categoría, haga clic en **CATEGORÍAS** en la parte derecha del cuadro **URL**. Aparecerá el cuadro de diálogo **Gestionar categorías**.

Seleccione **Agregar categoría** para crear una categoría y nombrarla como desee. A continuación, seleccione las URL de interés para la nueva Categoría. Para buscar direcciones URL, simplemente comience a escribir en el cuadro de búsqueda y la lista de direcciones URL se filtrará al texto de búsqueda.

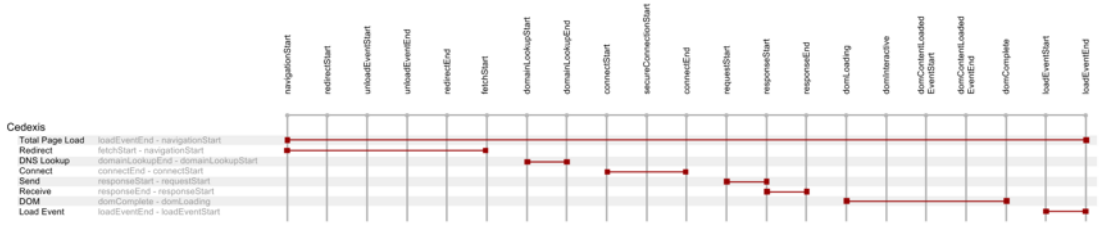
Cuando se hayan seleccionado todas las direcciones URL para la categoría, haga clic en el botón **Guardar** para completar la definición de **categoría**.

Datos de tiempo de navegación y tiempo de carga de página

La etiqueta Radar puede recopilar información detallada sobre el rendimiento de descarga de las páginas que implementan la etiqueta. La información de rendimiento de la API NavTiming se recopila de los navegadores que admiten la API (Chrome 6.5+, Firefox 8+, IE9+).

NetScaler muestra esta información en el portal del cliente, donde les permite ver el rendimiento que experimentan los usuarios finales reales al interactuar con sus páginas web.

A continuación se muestra un diagrama y una descripción de cada una de las métricas de carga de página que el Radar proporciona a través de la sincronización de navegación:



Medición	Descripción	Cálculo de sincronización de navegación
Carga total de página	La descarga completa de la página web y sus componentes correspondientes.	`loadEventEnd - navigationStart`
Redirigir	La hora inicial utilizada para redirigir a la página.	`fetchStart - navigationStart`
Búsqueda DNS	El tiempo necesario para completar la resolución DNS del URI de la página base.	`domainLookupEnd - domainLookupStart`
Conectar	Tiempo para realizar una conexión TCP, incluyendo SSL si se utiliza.	`connectEnd - connectStart`
Enviar	El tiempo de solicitud HTTP y respuesta de la página base inicial, excluyendo cualquier cuerpo del mensaje.Un buen indicador de latencia del servidor back-end.	`responseStart - requestStart`
Recibir	Tiempo necesario para recibir el código HTML del cuerpo del documento base.	`responseEnd - responseStart`
dom	El tiempo para descargar todos los medios, objetos que se llaman desde HTML base y cargarlos en el explorador.	`domComplete - domLoading`
Load (evento)	El tiempo para ejecutar cualquier JavaScript y renderizar la página dentro del explorador.	`loadEventEnd - loadEventStart`

Medición	Descripción	Cálculo de sincronización de navegación
Iniciar modelizado	La hora de inicio de procesamiento es el primer punto en el tiempo en que algo se puso a disposición de la pantalla.	Más tiempo agregado por Chrome/IE como una extensión a la API NavTiming.

Datos de repetición de vídeos

June 4, 2021

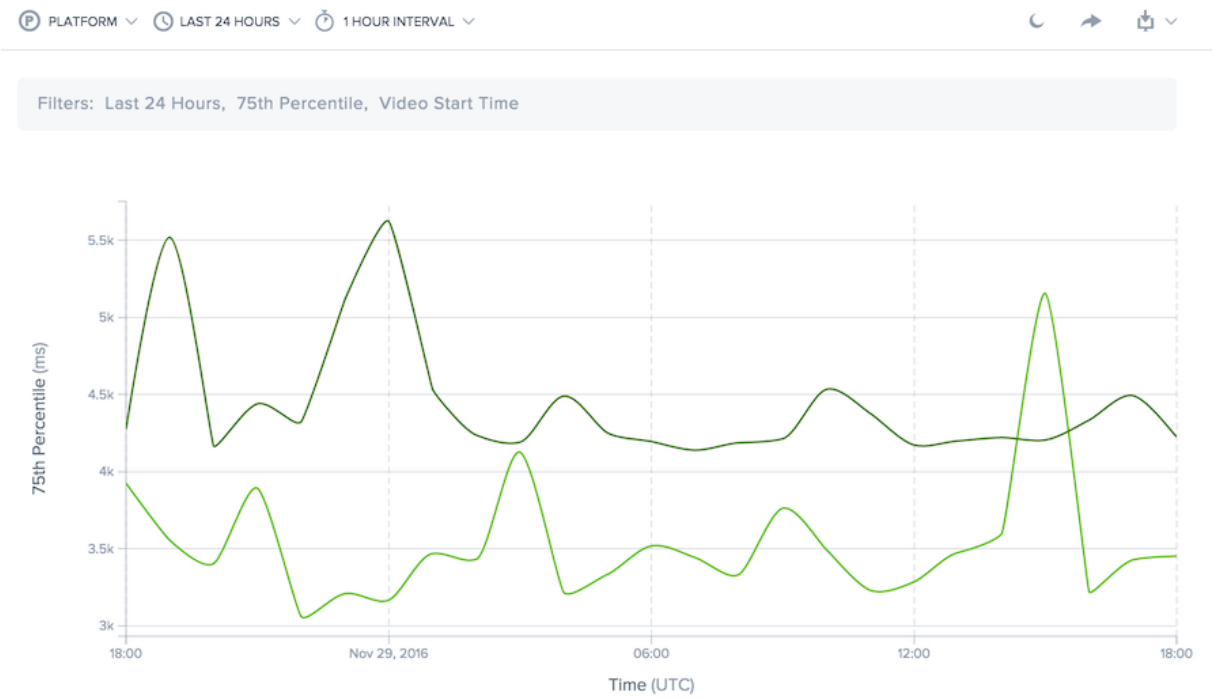
Cloud Platform Visualization recopila el rendimiento de la red de vídeo más pertinente y la calidad de los datos de experiencia para generar informes. La calidad del vídeo de la experiencia está directamente impulsada por la calidad de la entrega de fragmentos de vídeo. Openmix optimiza en función de las métricas de entrega de red Radar para proporcionar la mejor experiencia de visualización posible a los usuarios. Después de una breve descripción de los informes hay detalles sobre cómo pivotar, filtrar y personalizar los informes.

Informes de reproducción de vídeo

El menú **Datos de reproducción de vídeo** incluye los siguientes informes:

1. **Informe de rendimiento**: Experiencia de vídeo y datos de entrega a lo largo del tiempo.
2. **Informe de distribución estadística**: Variación en la experiencia de visualización de vídeo a lo largo del tiempo.
3. **Informe de comparación de histogramas** - Compare datos de entrega de fragmentos de vídeo con KPI de calidad de experiencia.

Informe de rendimiento

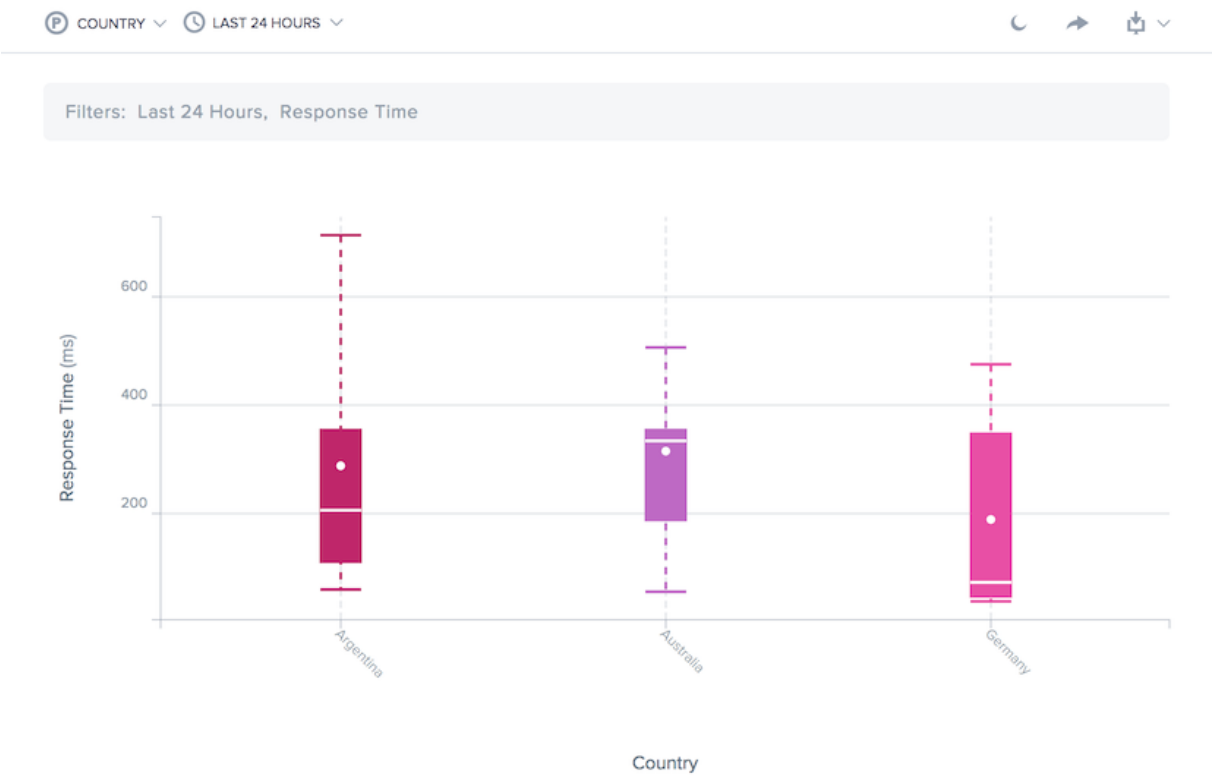


Este informe muestra la experiencia de visualización de vídeo a lo largo del tiempo. Le permite visualizar las tendencias de entrega a lo largo del tiempo, ver cuánto vídeo se está viendo y la calidad agregada de la experiencia de visualización.

Los datos se pueden ver con dimensiones que permiten la comparación de varios valores. Por ejemplo, los datos se pueden ver por dominio para comparar el rendimiento de la entrega en varios dominios de vídeo.

El período de tiempo para el informe se puede personalizar desde los últimos 60 minutos hasta 30 días en los últimos 13 meses.
Los datos se pueden filtrar por la plataforma que se utiliza para servir el contenido, el nombre del host y la ruta de los fragmentos de contenido o vídeo, la ubicación geográfica, la red o el agente de usuario del visor.

Informe de distribución estadística



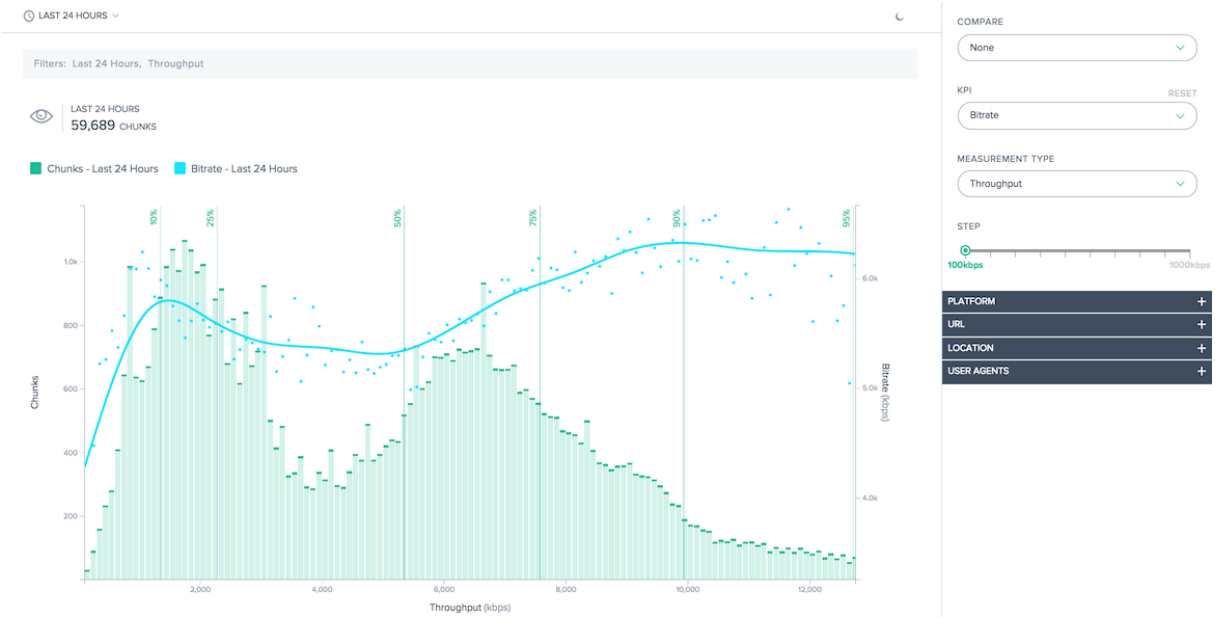
Este informe muestra la variación en la experiencia de visualización de vídeo a lo largo del tiempo. Le permite visualizar la forma en que se entrega el vídeo de manera consistente y comprender mejor las experiencias de visualización en toda la población de usuarios. El informe calcula el rendimiento del usuario en los percentiles 10, 25, 50, 75 y 95 y la media.

Al igual que el informe de rendimiento, los datos se pueden ver con dimensiones que permiten comparar varios valores. Por ejemplo, los datos se pueden ver por plataforma (proveedor de servicios o servidor) para comparar la consistencia de la entrega para varias plataformas.

El período de tiempo para el informe se puede personalizar desde los últimos 60 minutos hasta 30 días en los últimos 13 meses.

Los datos se pueden filtrar por la plataforma que se utiliza para servir el contenido, el nombre del host y la ruta de los fragmentos de contenido o vídeo, la ubicación geográfica, la red o el agente de usuario del visor.

Informe de comparación de histogramas



Este informe remarca las relaciones entre los datos de entrega de fragmentos de vídeo y los KPI de calidad de experiencia.

Hay dos funciones principales en este informe:

- El histograma muestra la frecuencia con la que se entregaron fragmentos de vídeo con un nivel de calidad especificado, ya sea Tiempo de respuesta o Rendimiento.
- Los KPI individuales pueden superponerse en el histograma. Las líneas trazan el KPI producido cuando se entregó un fragmento con el nivel de calidad especificado.

Por ejemplo, el histograma mostraría el rendimiento del fragmento medido por Radar. Es probable que los KPI muestren que la tasa de bits es mayor y que el rebúfer es menor cuando el rendimiento medido es mayor. En conjunto, estas funciones ayudan a cuantificar la relación entre la calidad de la entrega y la calidad de la experiencia producida para el espectador.

Si la generación predeterminada del informe no es suficiente, el tamaño del depósito del histograma puede personalizarse y se pueden seleccionar secciones específicas de la distribución para mostrarlas.

Además de relacionar histogramas con KPI, los datos se pueden comparar directamente. Se pueden seleccionar varios KPI para ver y los períodos de tiempo anteriores se pueden comparar para mostrar cambios en el rendimiento a lo largo del tiempo.

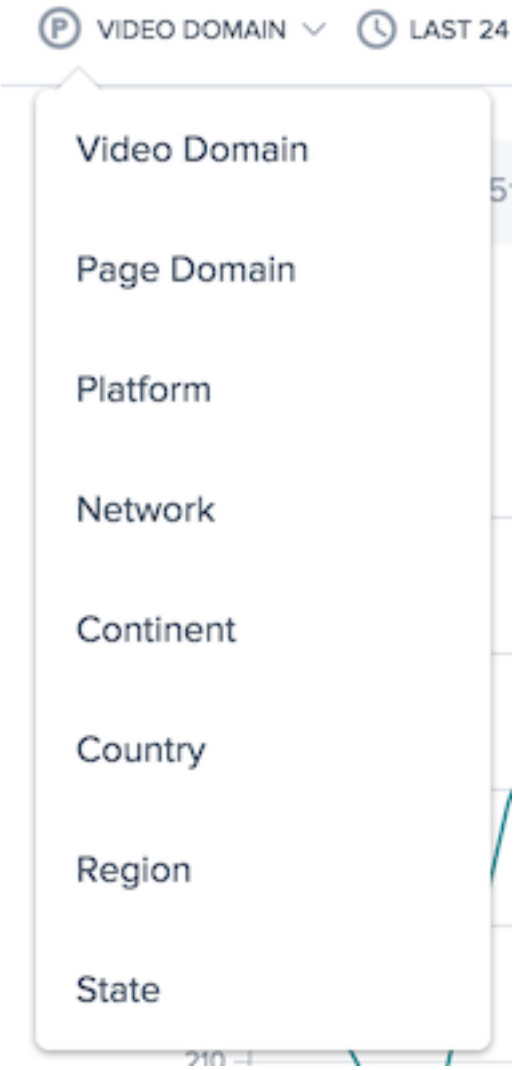
Los datos se pueden filtrar por la plataforma que se utiliza para servir el contenido, el nombre del host y la ruta de los fragmentos de contenido o vídeo, la ubicación geográfica, la red o el agente de usuario del visor.

Uso de informes de reproducción de vídeo

Para refinar y personalizar las vistas de informes para necesidades específicas de informes, utilice la siguiente funcionalidad en los informes Reproducción de vídeo de distribución estadística y rendimiento.

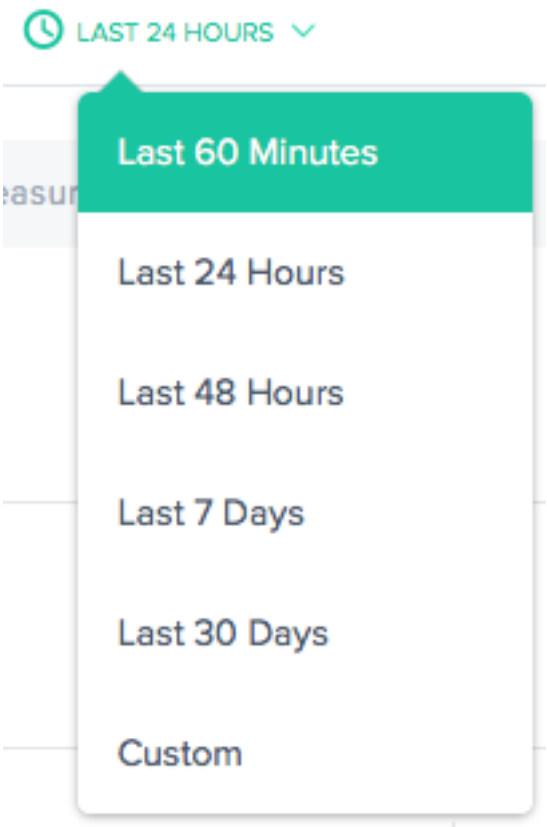
Además de las funciones estándar de los informes, como compartir informes, alternar en segundo plano, exportar datos y más, están disponibles las siguientes funciones:

Dimensión principal



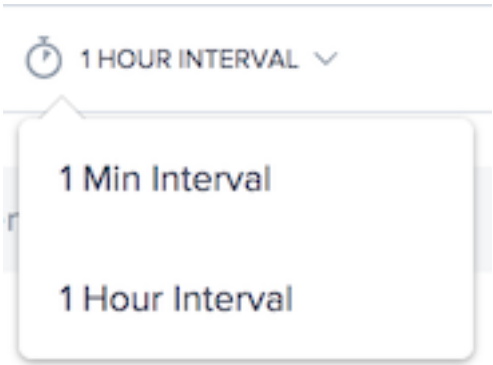
La dimensión principal del gráfico se selecciona mediante una lista de selección situada encima del gráfico. Utilice esto como un potente pivote en el informe para expresar los datos en términos de dominio de vídeo, dominio de página, plataforma, red (ASN), continente, país, región o estado.

Filtro: Rango de tiempo del informe



Los informes se pueden generar con un intervalo de tiempo de últimos 60 minutos, últimas 24 horas, últimas 48 horas, últimos 7 días, últimos 30 días o un rango personalizado. La vista predeterminada es las últimas 24 horas.

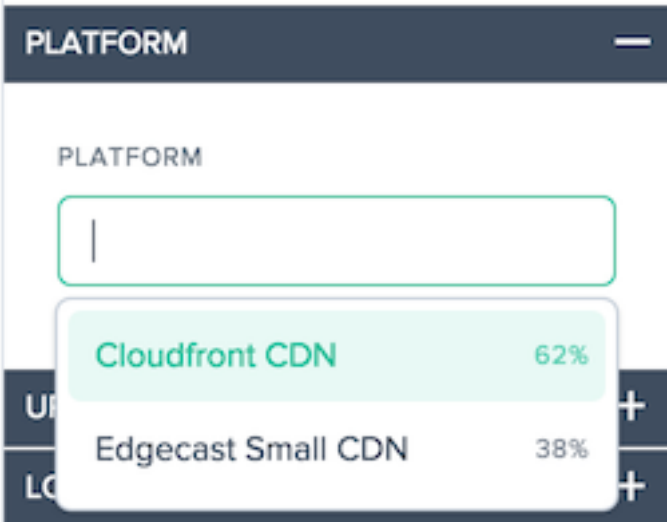
Intervalo de informe



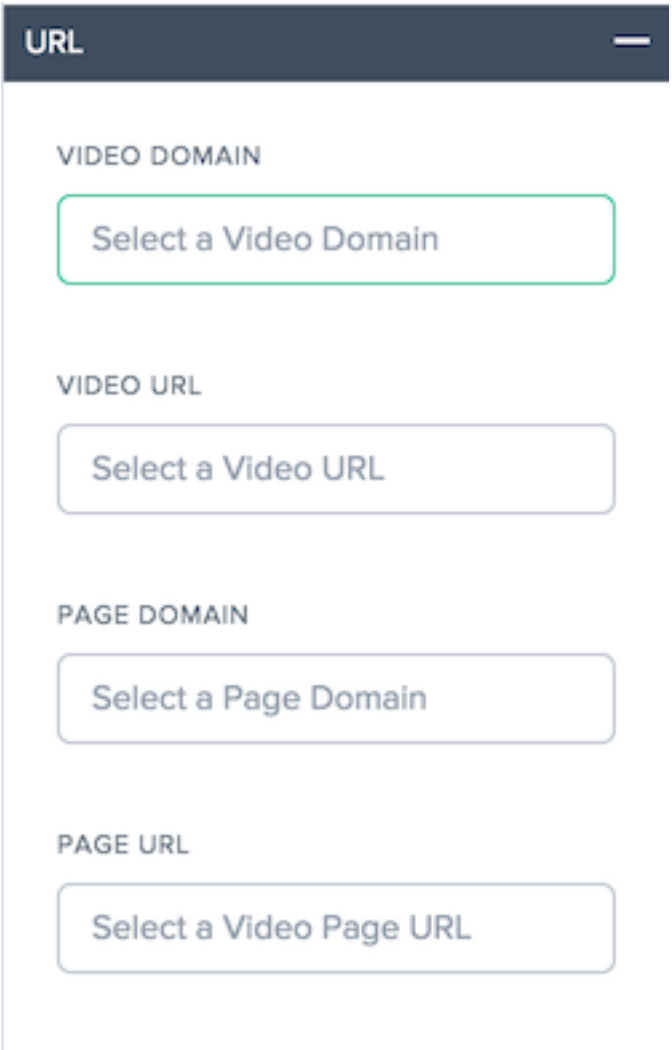
La dimensión principal del gráfico se selecciona mediante una lista de selección situada encima del gráfico. Esto permite generar informes granulares de datos de rendimiento.

Filtros: Potentes capacidades de profundización

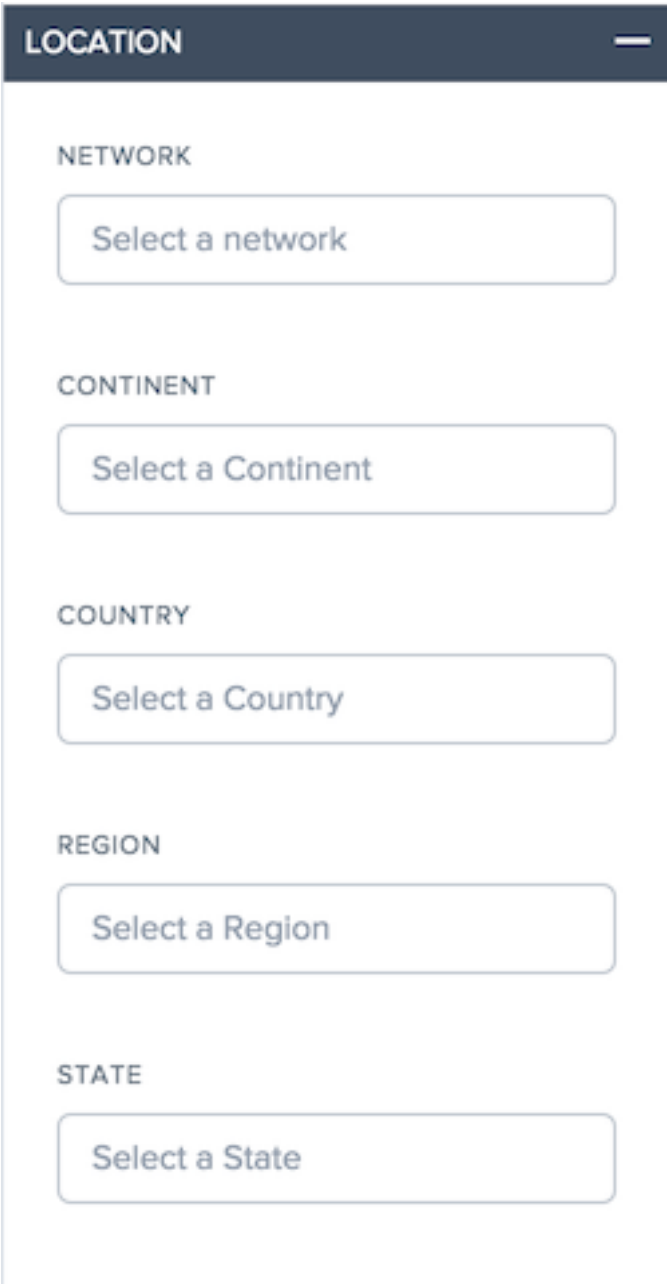
Los informes varían ligeramente en términos de qué filtros son apropiados en función de los datos. Los siguientes informes están disponibles en los informes de reproducción de vídeo:



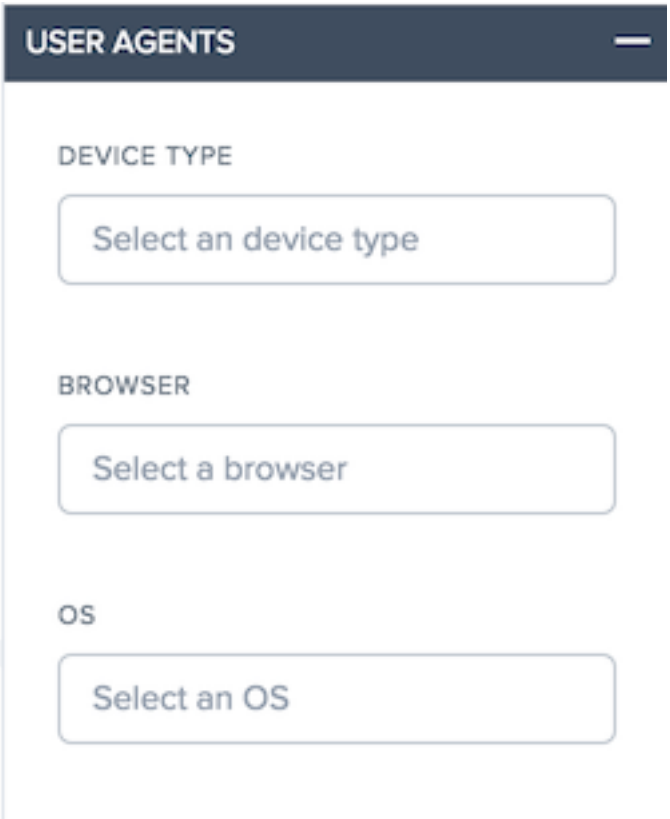
- **Plataforma** : seleccione una o Plataformas para filtrar, de forma predeterminada todas las plataformas se incluyen en el informe.



- **Dominio de vídeo** : seleccione uno o varios nombres de host en los que se alojan los vídeos; de forma predeterminada, todos los nombres de host se incluyen en el informe.
- **URL de vídeo** : seleccione una o más rutas para los vídeos, de forma predeterminada todas las rutas se incluyen en el informe.
- **Dominio de página** : seleccione uno o varios nombres de host en los que se hospedan las páginas; de forma predeterminada, todos los nombres de host se incluyen en el informe.
- **URL de página** : seleccione una o varias rutas para las páginas; de forma predeterminada, todas las rutas se incluyen en el informe.



- **Red**: Seleccione una o más redes (ASN) para incluir
- **Continente**: Seleccione uno o más continentes para incluir
- **País**: Seleccione uno o más países para incluir
- **Región**: Seleccione una o más regiones geográficas (cuando corresponda) para incluir
- **Estado**: Seleccione uno o más estados geográficos (cuando corresponda) para incluir

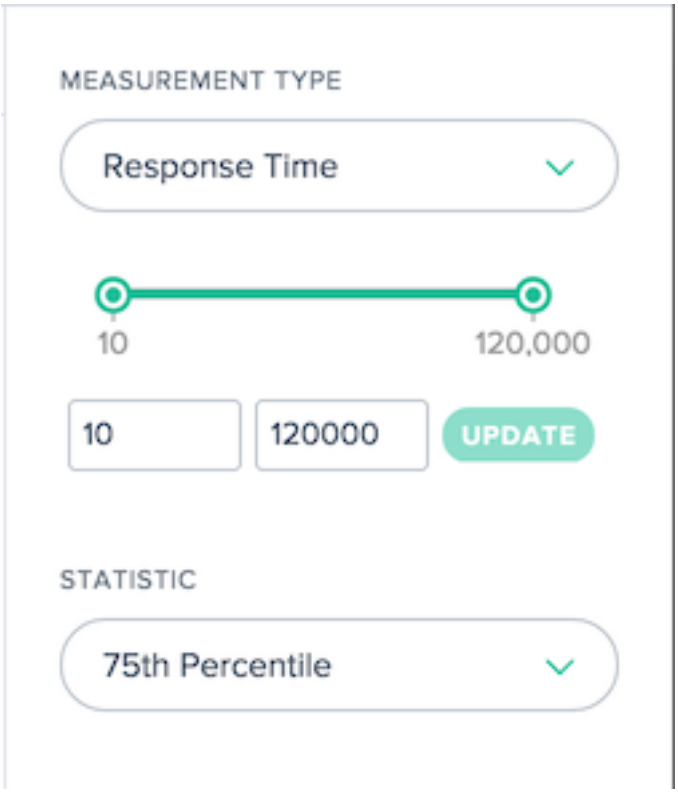


- **Agente de usuario**: Seleccione uno o más tipos de dispositivos, exploradores y/o tipos de SO para refinar aún más los datos de informes.

Uso del informe de rendimiento de reproducción de vídeo

Para refinar y personalizar el informe de rendimiento para necesidades específicas de informes, utilice la siguiente funcionalidad en el informe de rendimiento.

Filtros: Potentes capacidades de profundización



Los informes varían ligeramente en términos de qué filtros son apropiados en función de los datos. Los siguientes informes están disponibles en los informes de reproducción de vídeo:

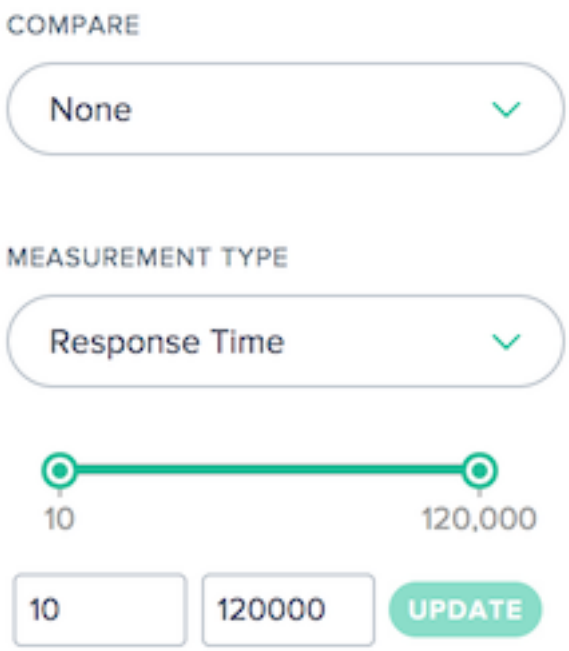
- **Tipo de medida**: Seleccione el tipo de medida que desea ver; el tiempo de respuesta se selecciona inicialmente.
- **Control deslizante de conteo** : filtra los datos por el número de medidas mínimo y máximo necesario para incluirlos en el informe.
- **Estadística**: Seleccione la medida estadística que desea ver.

Además de estos filtros específicos del informe, los filtros estándar de reproducción de vídeo están disponibles para personalizar los resultados.

Uso del informe de distribución estadística de reproducción de vídeo

Para refinar y personalizar el informe según necesidades específicas de informes, aplique la siguiente funcionalidad en el informe Distribución estadística.

Filtros: Potentes capacidades de profundización



Los informes varían ligeramente en términos de qué filtros son apropiados en función de los datos. Los siguientes informes están disponibles en los informes de reproducción de vídeo:

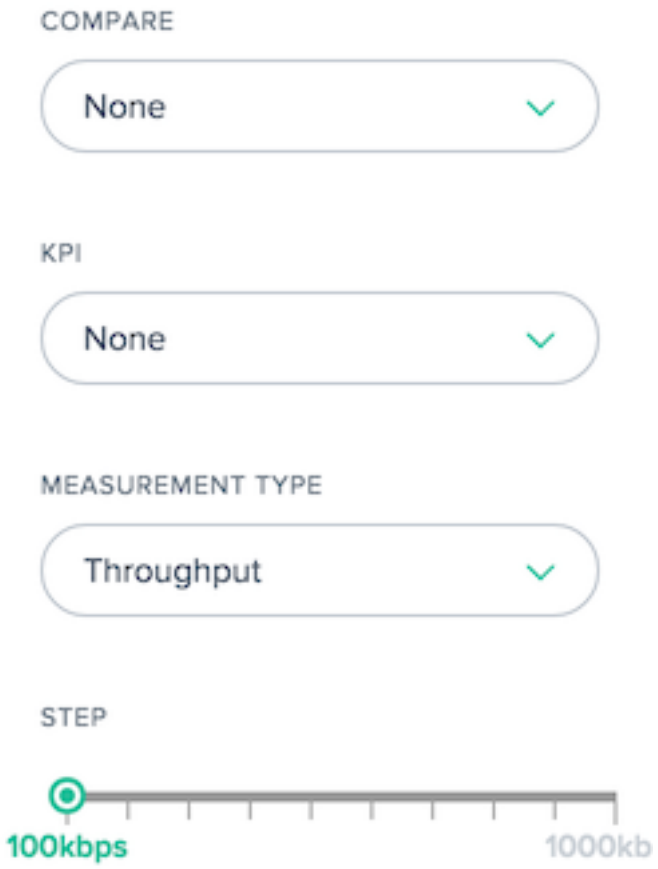
- **Comparar**: Seleccione el valor utilizado para crear una comparación en el informe. En función de la selección realizada, es necesario seleccionar los valores específicos utilizados para comparar. Las distribuciones resultantes se mostrarán lado a lado para que puedan compararse fácilmente.
- **Tipo de medida**: Seleccione el tipo de medida que desea ver; el tiempo de respuesta se selecciona inicialmente.
- **Control deslizante de conteo** : filtra los datos por el número de medidas mínimo y máximo necesario para incluirlos en el informe.

Además de estos filtros específicos del informe, los filtros estándar de reproducción de vídeo están disponibles para personalizar los resultados.

Uso del informe de comparación de histogramas de reproducción de vídeo

Para refinar y personalizar el informe según necesidades específicas de informes, aplique la siguiente funcionalidad en el informe Comparación de histogramas.

Filtros: Potentes capacidades de profundización



Los informes varían ligeramente en términos de qué filtros son apropiados en función de los datos. En los informes de comparación de histogramas se encuentran disponibles los siguientes elementos:

- **Comparar**: Seleccione el valor utilizado para crear una comparación en el informe. En función de la selección realizada, es necesario seleccionar los valores específicos utilizados para comparar. Los histogramas y los KPI resultantes se superpondrán unos encima de otros para que puedan compararse fácilmente.
- **KPI**: Seleccione el KPI que se grafica en relación con el tipo de medida del histograma.
- **Tipo de medida**: Seleccione el tipo de medida utilizado para rellenar el histograma.
- **Paso deslizante** : Establece el tamaño de los depósitos utilizados para generar el histograma.

Además de estos filtros específicos del informe, los filtros estándar de reproducción de vídeo están disponibles para personalizar los resultados.

Datos de repetición de vídeos

Los datos se recopilan utilizando las propiedades y eventos deElemento de vídeo HTML5los datos de calidad de experiencia y elAPI de Resource Timing para los datos de fragmentos de vídeo, desde los exploradores que admiten las API.

Los datos de vídeo se muestran en el portal, donde se pueden generar informes con información sobre la calidad de la experiencia del usuario final y el rendimiento de la entrega de la red.

A continuación se muestra un diagrama y una descripción de cada una de las métricas de vídeo que se recopilan:

Medición	Descripción
Tiempo de respuesta por fragmento	El tiempo que tardan los trozos en comenzar la entrega en función de las mediciones de tiempo de recursos (`responseStart – requestStart`)
Rendimiento por porción	La velocidad a la que se descargaron fragmentos de vídeo en función de las mediciones de tiempo de recursos. (kbps)
Velocidad de bits entregada	La tasa de bits por segundo del vídeo en función del tamaño de los fragmentos entregados. (kb)
Ratio de rebúfer	Porcentaje de tiempo dedicado al rebúfer durante la reproducción. (%)
Fallas de inicio de vídeo	El tiempo de solicitud HTTP y respuesta de la página base inicial, excluyendo cualquier cuerpo del mensaje.Un buen indicador de latencia del servidor back-end.
Hora de inicio del vídeo	Cantidad de tiempo que se tarda en iniciar la reproducción de vídeo después de que se haya realizado el intento de reproducción. (ms)

Datos de temporización de recursos

June 4, 2021

Información general

Los datos de sincronización de recursos ofrecen una visión eficaz del rendimiento de los recursos individuales de nivel de objeto de su sitio web.

Resource Timing ayuda a los clientes a ver el rendimiento de la red de los objetos a nivel de página, en función de los datos que proporcionamos sobre el tiempo de conexión, el tiempo de descarga y los diferentes tiempos de respuesta. Ejemplos de objetos de nivel de página son, imágenes, archivos JavaScript, llamadas a API, etc. Ofrece a los clientes una mejor visibilidad de las prestaciones a nivel de página. El resultado final es que los clientes pueden gestionar mejor su entrega y garantizar una mejor calidad general de la experiencia del usuario.

Las siguientes secciones le guiarán por la configuración, la descripción de los datos y el informe de los datos de temporización de recursos.

Configuración de temporización de recursos

La interfaz de usuario del portal le permite introducir directamente los ajustes para la configuración de Resource Timing como una alternativa a la codificación JSON.

Nota: Aunque la configuración a través de la codificación JSON todavía está disponible, se recomienda encarecidamente que utilice la interfaz de usuario para la configuración.

Navegación

En el panel de navegación izquierdo, elija Impact -> Datos de temporización de recursos -> Configuración de temporización de recursos.

Configuración por primera vez

- Seleccione **Iniciar ahora** en la página de apertura para empezar.
- Se abre un cuadro de diálogo **Configuración predeterminada** para incluir o excluir recursos e introducir una frecuencia de muestreo.

Valores de configuración predeterminados Los valores de configuración predeterminados son los valores mínimos necesarios para comenzar. Hay tres opciones de configuración predeterminadas principales:

- Recursos para incluir y excluir
- Frecuencia de muestreo
- Detección predeterminada del proveedor

Recursos para incluir o excluir Esta función le permite incluir o excluir recursos específicos de los que recopilar datos de temporización. Si se deja en blanco, todos los recursos se incluyen de forma predeterminada (es decir, no se excluye nada).

Puede introducir recursos como, por ejemplo, un nombre de archivo, una extensión de nombre de archivo, un nombre de carpeta, una ruta de archivo o incluso una cadena. Cualquier cosa contenida en la cadena se recogerá como un recurso.

Presione **Entrar** o la tecla **Retorno** cada vez que introduzca un nombre de recurso para enviarlo. Si especifica recursos específicos en el campo **Incluir**, solo se incluirán esos recursos y se excluirán todos los demás recursos. Para excluir recursos específicos, introdúzcalos en el campo **Excluir** y se incluirá todo lo demás. Incluso puede escribir una lógica de expresiones regulares personalizada para personalizar el proceso de inclusión o exclusión.

Frecuencia de muestreo La **frecuencia de muestreo** le permite introducir una pequeña muestra de visitantes de los que desea recopilar datos de IRT. Introduzca un valor entre 0 y 100 (tomado como porcentaje). Idealmente, debe introducir el porcentaje más bajo para la tasa de muestreo, un valor que sea suficiente para recopilar el número requerido de mediciones de temporización de recursos.

Nota: La recopilación de datos de temporización de recursos pone una carga pesada en el sistema. Esta función es para que los clientes muestreen datos, y no está diseñada para recopilar datos para cada sesión de Radar.

Precaución: Para los clientes con un alto volumen de datos, comience con una frecuencia de muestreo del 1%. Aumente lentamente hasta que se alcance una tasa estadísticamente útil. Una frecuencia de muestreo alta puede provocar una sobrecarga del servidor, ralentizar o incluso un bloqueo.

Pasos para la configuración de la frecuencia de muestreo por primera vez

1. Comience con una frecuencia de muestreo del 1%. Espere 24-48 horas hasta que reciba algunas mediciones.
2. Compruebe el **gráfico IRT** para ver si tiene un aspecto suave en varios activos.
3. En caso afirmativo, deje la frecuencia de muestreo en este valor, a menos que el cliente tenga tráfico web alto.
4. Alternativamente, si el gráfico parece recortado debido al bajo volumen de datos, suba lentamente.
5. Repita todos los controles y siga aumentando la tasa lentamente (idealmente cada 24-48 horas) hasta que reciba datos suficientes (alrededor del 10%).
6. Para los clientes con tráfico web bajo, puede subir más del 10%. Pero por cada pequeño aumento, asegúrese de realizar todas las comprobaciones mencionadas.

Seleccione **Siguiente** para ir al cuadro de diálogo **Configuración de detección de proveedor predeterminada**.

Detección predeterminada del proveedor La detección del proveedor le permite identificar el proveedor o la plataforma desde donde se sirve el recurso. Escriba un nombre de host configurado para detectar el proveedor que sirve el recurso. Puede introducir varios nombres de host y configurar la detección de proveedores para cada uno de ellos individualmente. Consulte la sección Detección de proveedores para obtener información sobre cómo configurar la detección de proveedores.

Seleccione **Completar** para completar la configuración por primera vez.

Sitios

Los **datos de temporización de recursos** se configuran en torno a tres áreas principales:

1. **Sitios**
2. **Configuración**
3. **Detección de proveedores**

- Desde el panel de navegación izquierdo, vaya a **Impact -> Datos de temporización de recursos -> Temporización de recursos**.
- Se abrirá la página **Sitios** en **Datos de temporización de recursos**.

Introduzca el nombre de host del sitio desde el que desea recopilar datos de temporización de recursos. En **Sitios**, encontrará la lista de nombres de host que ya están en el sistema. Si no encuentra el sitio requerido (nombre de host), puede introducirlo haciendo clic en el botón **Agregar**. El **cuadro de diálogo Agregar sitio** le permite agregar un nuevo sitio para configurar los datos de temporización de recursos en.

Configuración

Acceda a **Impacto > Datos de temporización de recursos > Configuración de temporización** de recursos en el menú de navegación lateral del Portal. La página **Sitios** se abre en **Datos de temporización de recursos**.

En la barra de navegación superior, elija **Configuración**.

Puede agregar una nueva configuración haciendo clic en el botón Agregar en la esquina superior derecha de la página.

Nota: También puede ver una lista de configuraciones, incluida la configuración predeterminada en la página. En lugar de agregar una nueva configuración, puede seleccionar una configuración predeterminada o modificar una existente de la lista.

Agregar configuración

Para agregar una nueva configuración, haga clic en el botón **Agregar** en la esquina superior derecha de la página.

Se abrirá el cuadro de diálogo **Agregar configuración de tiempo de recurso**. Esto le permite introducir un nuevo **nombre**de configuración, agregar **recursos para incluir o excluir**y agregar la **frecuencia de muestreo**.

Modificar configuración

Para modificar una configuración existente, seleccione el botón **Modificar configuración** junto al nombre de configuración.

Detección de proveedores

La detección del proveedor determina qué plataforma maneja una solicitud de un dominio cuando ese dominio está equilibrado de carga detrás de Openmix. Se recomienda que todos los clientes que tengan habilitados los datos de temporización de recursos, configuren los servicios de detección de proveedores.

- Para configurar la detección de proveedores, vaya a **Impact > Datos de temporización de recursos > Configuración de temporización de recursos** en el panel de navegación izquierdo.
- Se abrirá la página **Sitios** en **Datos de temporización de recursos**. En la barra de navegación superior, elija **Detección de proveedor**.

Haga clic en el botón Agregar en la esquina superior derecha de la página.

En el cuadro de diálogo **Agregar configuración de detección de proveedor**, escriba lo siguiente.

Nombre de configuración

Introduzca un nombre para la configuración. El nombre no puede contener espacios ni caracteres especiales, y debe ser único.

Nombre de host

Introduzca el nombre de host para el que desea configurar la detección del proveedor. Puede introducir varios nombres de host y especificar métodos de detección para cada uno de ellos individualmente.

Método de detección

El método de detección implica especificar el tipo de objeto de prueba (ya sea estándar o personalizado) y la ruta (al objeto de prueba) para cada nombre de host que haya introducido.

Objetos de prueba estándar En el caso de objetos de prueba estándar, la ruta se puede especificar como, **/provider-detection/platform.html** y **/provider-detection/platform.png**. Para esta configuración, **/provider-detection/** sería su ruta de directorio.

Nota: No es obligatorio introducir la ruta descrita anteriormente. Sin embargo, para cualquier ruta de acceso que introduzca, asegúrese de que los archivos **platform.html** y **platform.png** se encuentran en la ruta de acceso del directorio.

Objetos de prueba personalizados En el caso de objetos de prueba personalizados, debe asegurarse de que los objetos de prueba se encuentran en la ruta exacta que introduzca. Por ejemplo, para el nombre de host `foo.com` y la ruta de acceso `static/bar.css`, la dirección URL `http://foo.com/static/bar.css` debe ser válida.

Encabezados

Encabezado de plataforma Si selecciona **Encabezado de plataforma**, asegúrese de que `X-CDN-Forward: <CDN name>` se envía el en los objetos de prueba. Si no `X-CDN-Forward: <CDN name>` se encuentra en los encabezados de respuesta, el cliente pasa a la siguiente prueba, que se puede especificar mediante **Personalizado**.

Personalizado Si selecciona **Personalizado**, asegúrese de que la expresión regular que introduzca coincida exactamente con uno de los encabezados de respuesta de la CDN.

Si agrega varios encabezados de respuesta, cada uno de ellos se prueba con las expresiones regulares en el mismo orden que se introdujo en el portal.

Haga clic en **Crear** para completar el proceso. Ahora verá la configuración recién creada en la lista de **Detección de proveedores**. Haga clic en los iconos de edición o eliminación si desea modificar la configuración o eliminarla.

Su configuración ya está completa. Para configurar la Detección de proveedores alternativamente mediante la codificación JSON, póngase en contacto con su representante de cuenta.

Descripciones de Medición de Temporización de Recursos

En la siguiente tabla se muestran las mediciones de temporización de recursos que se recopilan.

Medición	Descripción	Cálculo de temporización de recursos
Hora de búsqueda de DNS	El tiempo necesario para la resolución DNS del recurso. Se conoce como la fase DNS.	`domainLookupEnd – domainLookupStart`
Hora de conexión TCP	El tiempo que tarda un explorador en establecer la conexión con un servidor. Conocida como la fase TCP.	`connectEnd – connectStart`
Tiempo de espera para el primer byte (TTFB)	TTFB es la cantidad de tiempo que un explorador espera antes del inicio de la recepción del recurso.	`responseStart – startTime`
Tiempo de ida y vuelta (RTT)	Tiempo desde el inicio de la solicitud hasta el inicio de la respuesta. Se conoce como la fase de solicitud.	`responseStart – requestStart`
Tiempo de espera	La diferencia entre el inicio de la respuesta y el final de la respuesta. Conocida como la fase de respuesta. La respuesta suele ser de un servidor, caché o recurso local.	`responseEnd – responseStart`
Duración	El tiempo total desde el inicio del proceso hasta la recepción completa del recurso.	`responseEnd – startTime`

Obtenga más información enhttps://www.w3.org/TR/resource-timing-1/#process

Informes de temporización de recursos

El menú **Temporización de recursos** incluye los siguientes informes:

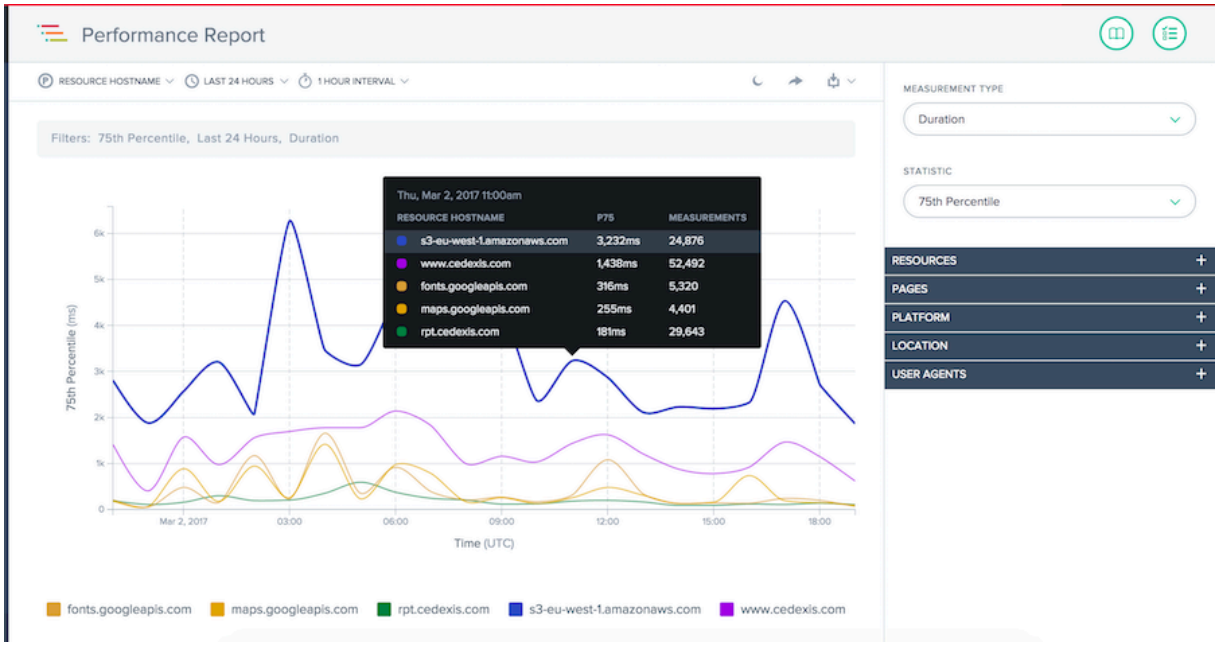
1. **Informe de rendimiento**: Datos de medición de temporización de recursos a lo largo del tiempo.
2. **Informe de distribución estadística**: Vista de los datos de temporización de recursos a través de una vista de informes de distribución estadística.

Informe de rendimiento

El informe proporciona información sobre los datos de rendimiento de la temporización de recursos a lo largo del tiempo por valor seleccionado.

Vista de informes predeterminada:

1. Dimensión: Nombre de host de recurso
2. Medida: Duración
3. Rango de tiempo: últimas 24 horas.

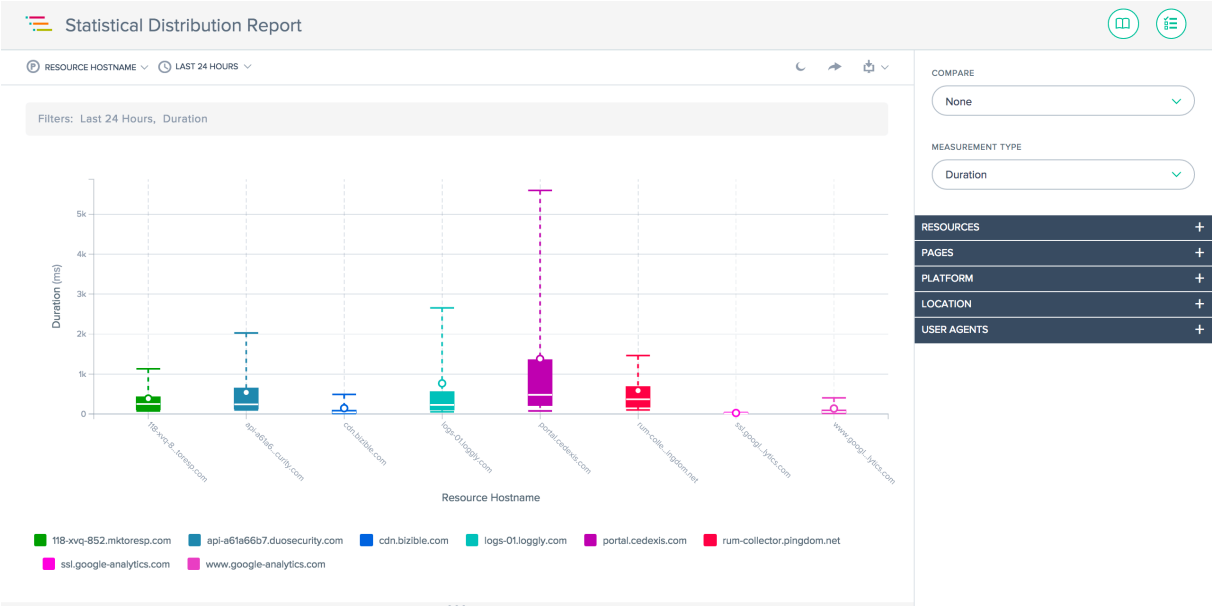


Informe de distribución estadística

Este informe muestra la distribución estadística de Resource Timing. El informe da una idea de cuántas mediciones se recogieron por valor de recurso. Puede filtrar según Recursos, Página, Plataforma, Ubicación y Agente de usuario, cambiar entre tipos de medida y ejecutar comparaciones entre detalles específicos de página, ubicación y agente de usuario.

Vista de informes predeterminada:

1. Dimensión: Nombre de host de recurso
2. Medida: Duración
3. Rango de tiempo: últimas 24 horas.

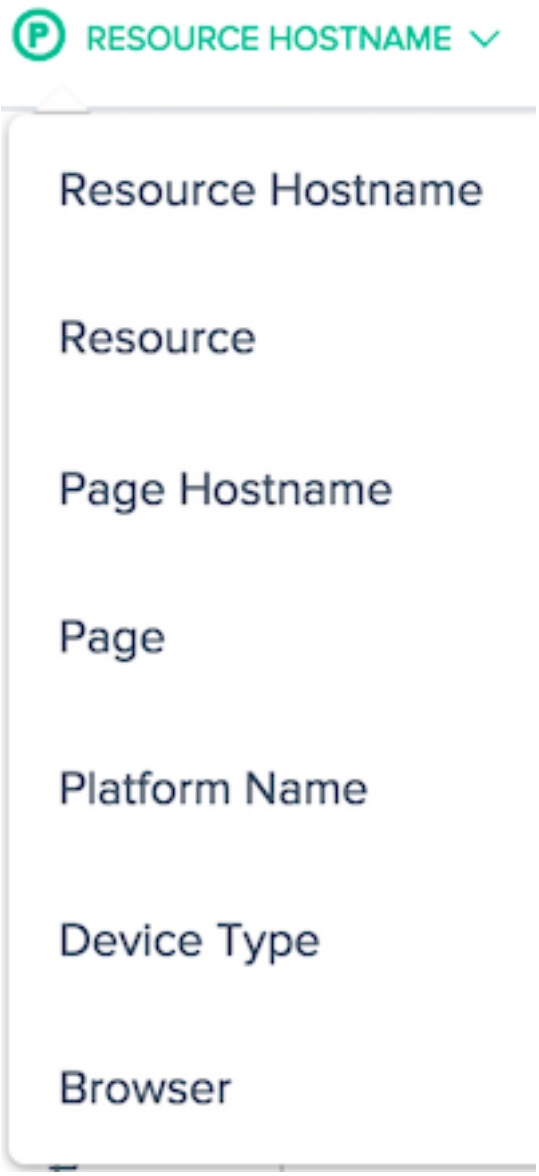


El gráfico de bigotes

Uso de los informes

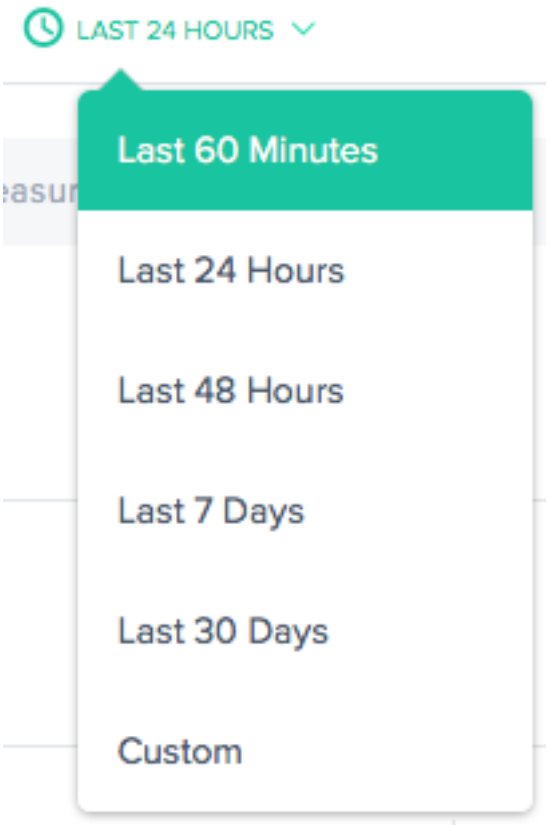
Para refinar y personalizar las vistas de informes para necesidades específicas de informes, utilice la siguiente funcionalidad en los informes de rendimiento y distribución estadística. Además de las funciones estándar de los informes, como compartir informes, alternar en segundo plano, exportar datos y más, están disponibles las siguientes funciones:

Dimensión principal



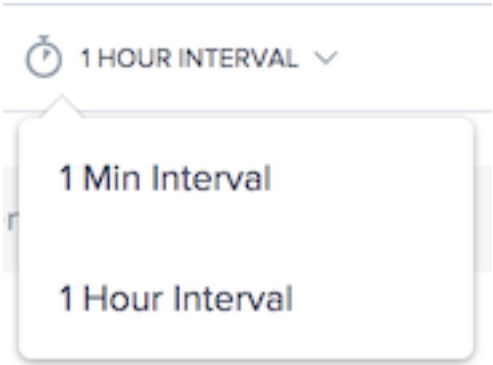
La dimensión principal del gráfico se selecciona a través de un menú sobre el gráfico. Puede utilizarlo como un potente pivote en el informe para expresar datos en términos de nombre de host de recurso, nombre de host de página, página y nombre de plataforma.

Filtro: Rango de tiempo del informe



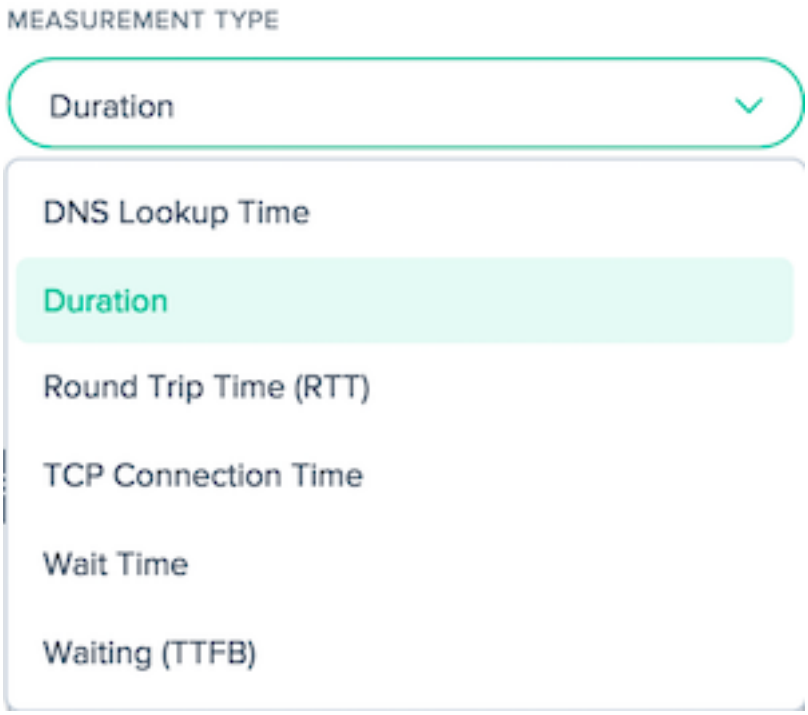
Los informes se pueden generar con un intervalo de tiempo de últimos 60 minutos, últimas 24 horas, últimas 48 horas, últimos 7 días, últimos 30 días o un rango personalizado. La vista predeterminada es las últimas 24 horas.

Intervalo de informe



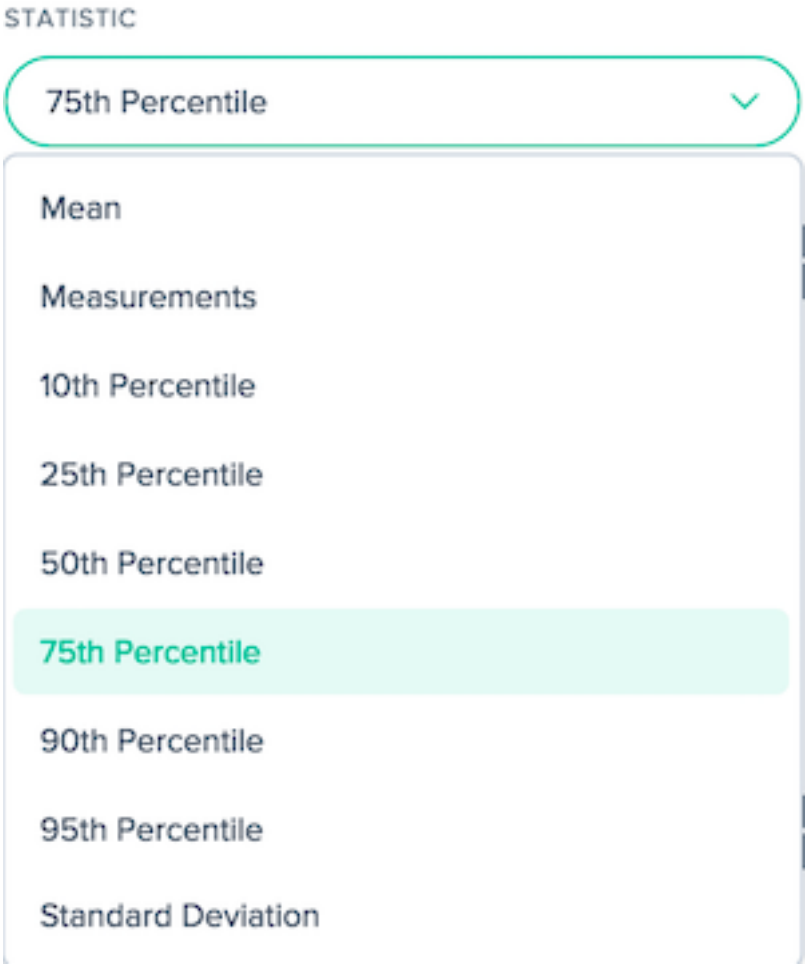
Seleccione el intervalo de tiempo en el que desea ver el gráfico de tendencias. Dependiendo del intervalo de fechas que esté visualizando, puede ver el gráfico en intervalos de un minuto, una hora o un día.

Tipos de medición



Seleccione el tipo de medida con el que desea ver la temporización del recurso. Elija entre Duración, Tiempo de búsqueda DNS, Tiempo de ida y vuelta (RTT), Tiempo de conexión TCP, Tiempo de espera y Espera (TTFB).

Seleccione una medida estadística para ver los datos.



Filtros: Potentes capacidades de obtención de detalles

Los informes varían ligeramente en términos de qué filtros son apropiados en función de los datos. Las siguientes opciones de filtro están disponibles en los informes:

Nombre del host del recurso:

RESOURCE HOSTNAME

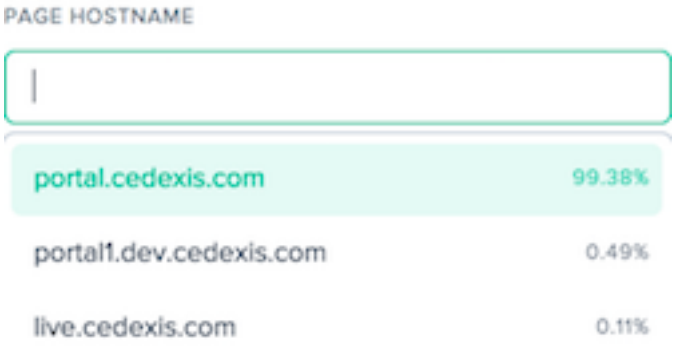
portal.cedexis.com	56.84%
www.google-analytics.com	14.7%
cdn.bizible.com	9.9%
logs-01.loggly.com	9.02%
118-xvq-852.mktoresp.com	7.46%
rum-collector.pingdom.net	2.02%
api-a61a66b7.duosecurity.com	0.05%
ssl.google-analytics.com	0.01%
api-ext.intricately.com	0.01%

Recursos:

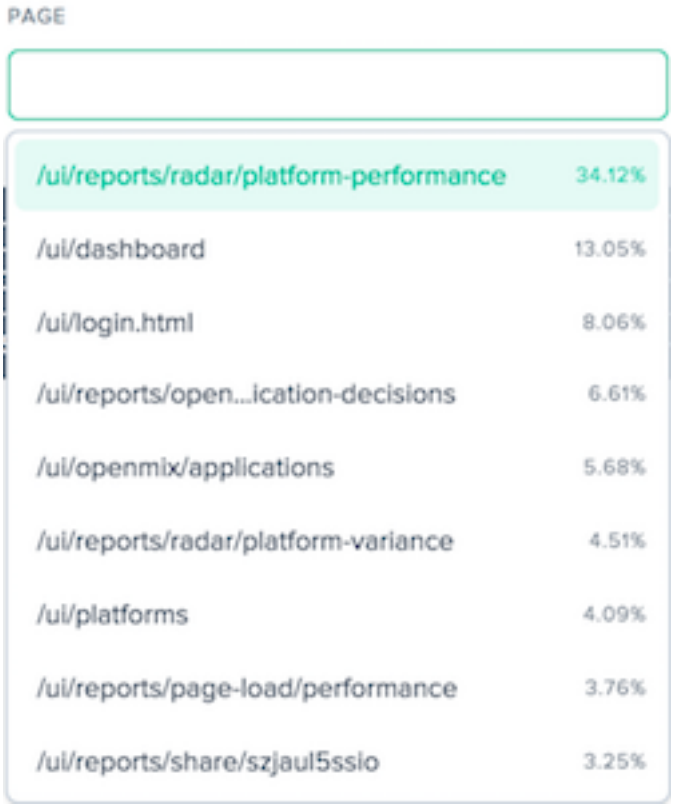
RESOURCE

/collect	11.92%
/m/ipv	9.25%
/inputs/9260e0ca...-24a42dc71056.gif	9.02%
/api/v2/reporting/radar.json	5.73%
/webevents/visitWebPage	5.67%
/api/v2/reporting/openmix.json	4.67%
/r/collect	2.77%
/provider-detection/platform.htm	2.25%
/api/v2/reporting/session.json	2.03%

Nombre de host de página:

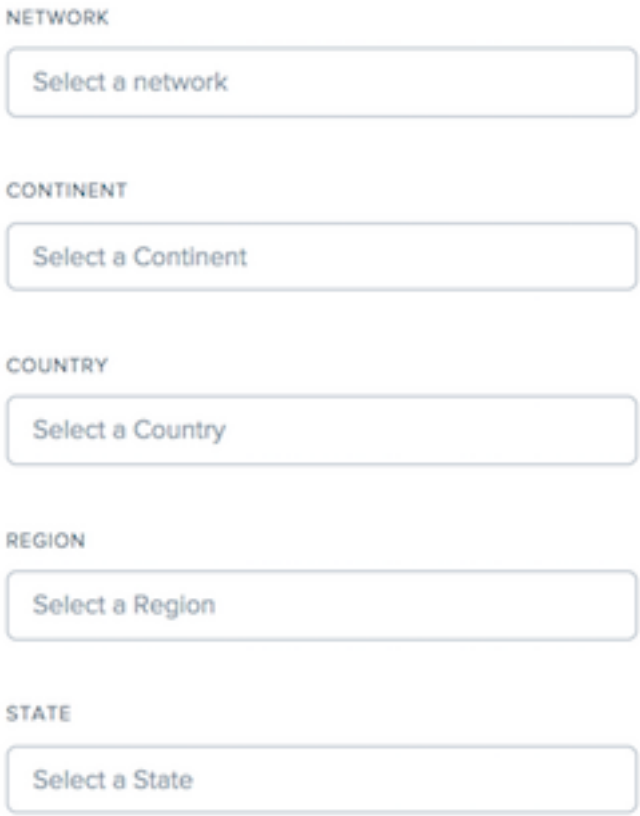


Página:

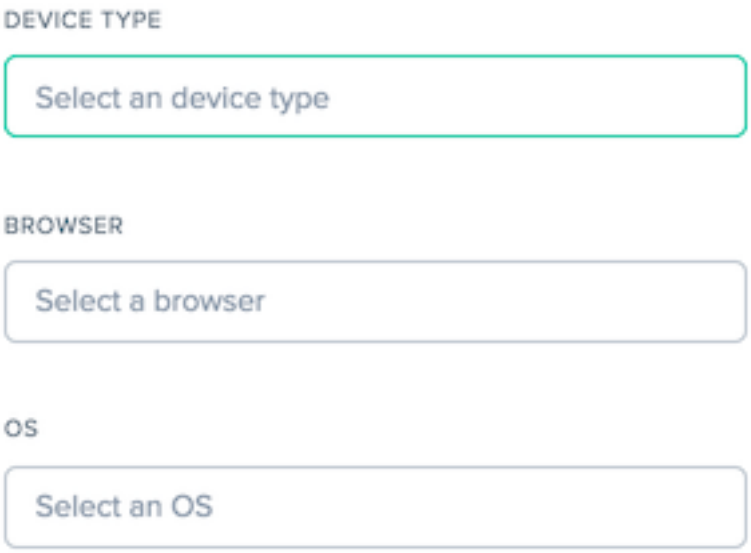


Nombre de la plataforma:

Ubicación: Red, Continente, País, Región y Estado:



Agentes de usuario: Tipo de dispositivo, explorador e IOS:

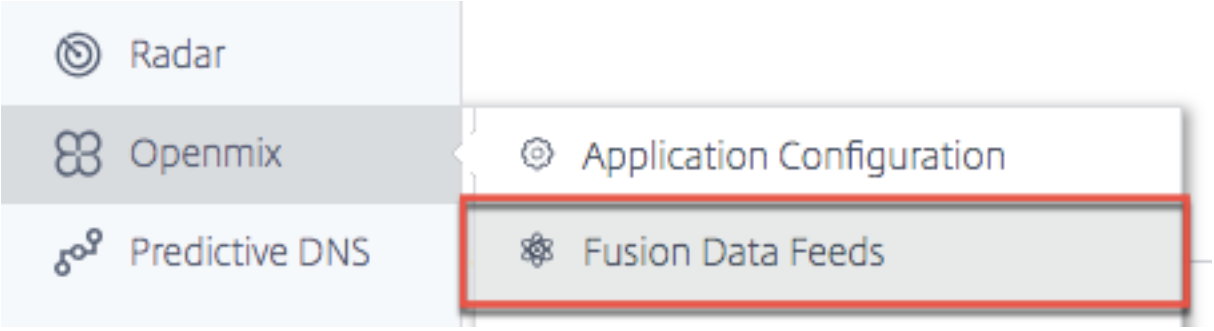


Integraciones de Fusion

September 13, 2023

Además de los datos de Radar y Sonar, Openmix puede utilizar datos de terceros en sus criterios de decisión. Por ejemplo, puede integrar un servicio de supervisión sintética existente que ya utilice. O puede tomar decisiones basadas en costes utilizando datos de uso actualizados de su proveedor de CDN.

Menú Fusion



Se puede acceder a Fusion Data Feeds desde el menú de navegación, en **Openmix**.

Por ejemplo, algunas fuentes de datos comunes de Fusion que funcionan con aplicaciones Openmix:

1. **Disponibilidad del servidor** : ingiere datos de proveedores externos como CatchPoint, Rigor y Pingdom para determinar la accesibilidad de un host o aplicación específico.
2. **Supervisión de servidores** : las métricas de proveedores como Rackspace y New Relic permiten a Openmix tener en cuenta las métricas de tiempo de ejecución del servidor, como el uso de memoria, el consumo de CPU, el espacio libre en disco y la latencia de red en la decisión de enrutamiento. Openmix puede utilizar las métricas para tomar decisiones de enrutamiento de encendido/apagado o para realizar cambios graduados de enrutamiento mediante la descarga de tráfico de un servidor cargado.
3. **Control de costes de CDN** : ingiere estadísticas de ancho de banda y uso de todos los CDN principales y hace que estos datos estén disponibles en tiempo real en aplicaciones Openmix en decisiones de enrutamiento de impacto.
4. **Fuentes de datos personalizadas definidas por el cliente** : cualquier dato en un punto final que proporcione se puede ingerir y poner a disposición en una aplicación Openmix personalizada para su uso en la decisión de enrutamiento.

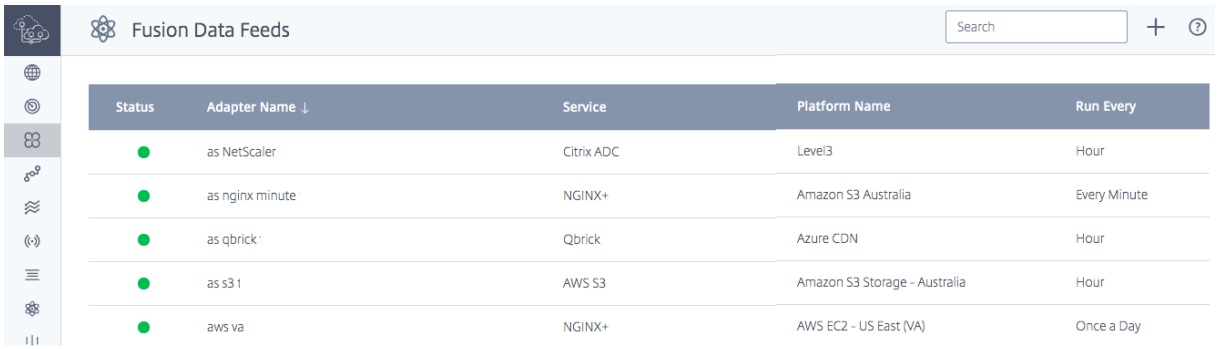
Integraciones de Fusion

Servicio	Tipo
Akamai	Ancho de banda de CDN, Uso de CDN
AWS CloudFront	Uso de CDN
AWS CloudWatch	Métricas de Instancia
COMO ELB	Métricas del equilibrador de carga
AWS S3	Fuente de datos personalizada
Azure	Métricas de Instancia
Catchpoint	Alertas
CDNetworks	Ancho de banda de CDN, Uso de CDN
ChinaCache	Ancho de banda CDN
ChinaNetCenter	Ancho de banda CDN
NetScaler	Fuente de datos personalizada
Datadog	Alertas
Edgecast	Ancho de banda de CDN, Uso de CDN
Fastly	Uso de CDN
Fusión directa	Fuente de datos personalizada
Highwinds	Uso de CDN
HTTP OBTENER	Fuente de datos personalizada
HTTP GET con disponibilidad	Fuente de datos personalizada
JSON	Fuente de datos personalizada
Keynote	Monitor web
Level3	Ancho de banda de CDN, Uso de CDN
Limelight	Uso de CDN
CDN máximo	Ancho de banda de CDN, Uso de CDN
Nueva reliquia Apdex	Puntuación de la aplicación
Monitoreo del nuevo servidor de reliquia	Métricas de Instancia
NGINX	Métricas del equilibrador de carga
NGINX+	Métricas del equilibrador de carga

Servicio	Tipo
Pingdom	Monitor web
Qbrick	Uso de CDN
Rackspace	Métricas de Instancia
Rigor	Monitor web
SFR	Ancho de banda de CDN, Uso de CDN
Ping TCP	Monitor web
Touchstream	Monitorización de vídeo

Fuentes de Fusion

La siguiente pantalla muestra todas las Fusion Data Feeds configuradas. La lista proporciona una visión general de las fuentes de datos y el estado actual.



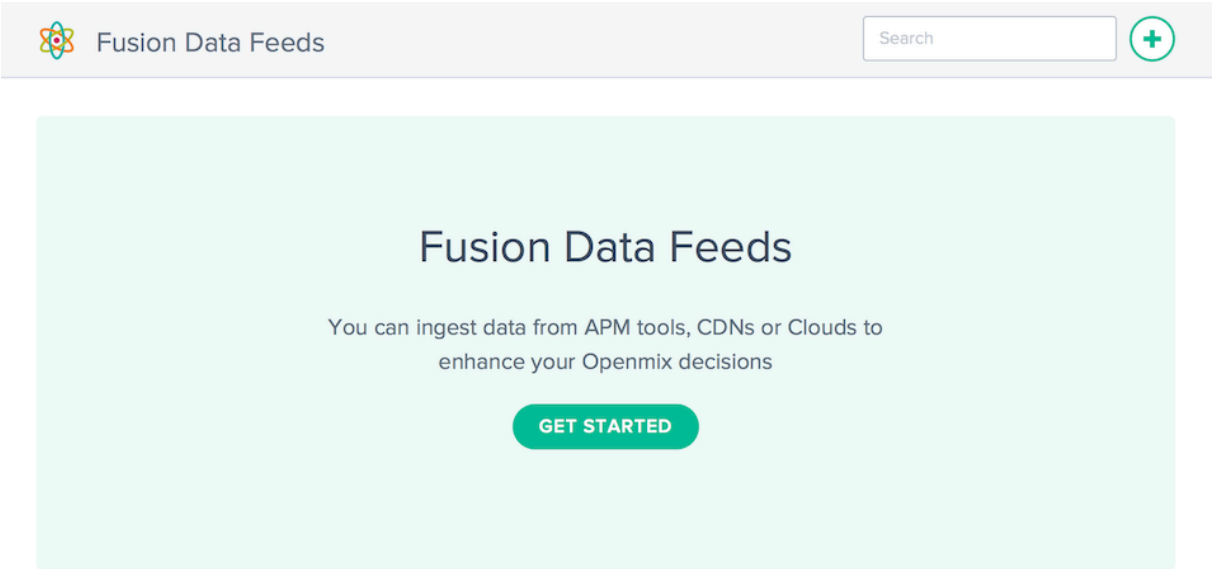
Las columnas proporcionan la siguiente información:

Encabezado	Descripción
Estado	El estado actual de la fuente de datos. El estado muestra: + verde, lo que significa que el feed está recuperando correctamente los datos del servicio; + amarillo, significa que el feed está esperando que los datos se recuperen del servicio; o + rojo, lo que significa que el feed no se puede recuperar desde el servicio
Nombre de fuente de datos	Nombre dado en el feed de datos. Opcional, será predeterminado en “Service - Platform Name”si no se especifica.

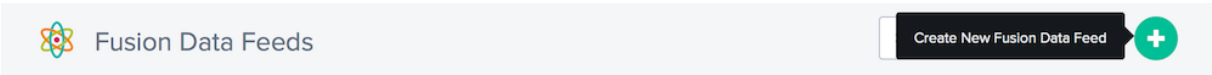
Encabezado	Descripción
Servicio	Nombre del servicio que utiliza el feed de datos.
ID	El ID de la fuente de datos. Esto es necesario para acceder a Fusion a través de la API.
Nombre de la plataforma	El nombre de la Plataforma asociada a la fuente de datos.
Ejecutar cada	Con qué frecuencia se actualiza la fuente de datos desde el servicio.

Creación de fuentes de datos

Si no se configuran Fusion Data Feeds, una pantalla de bienvenida le pedirá que cree una fuente de datos.

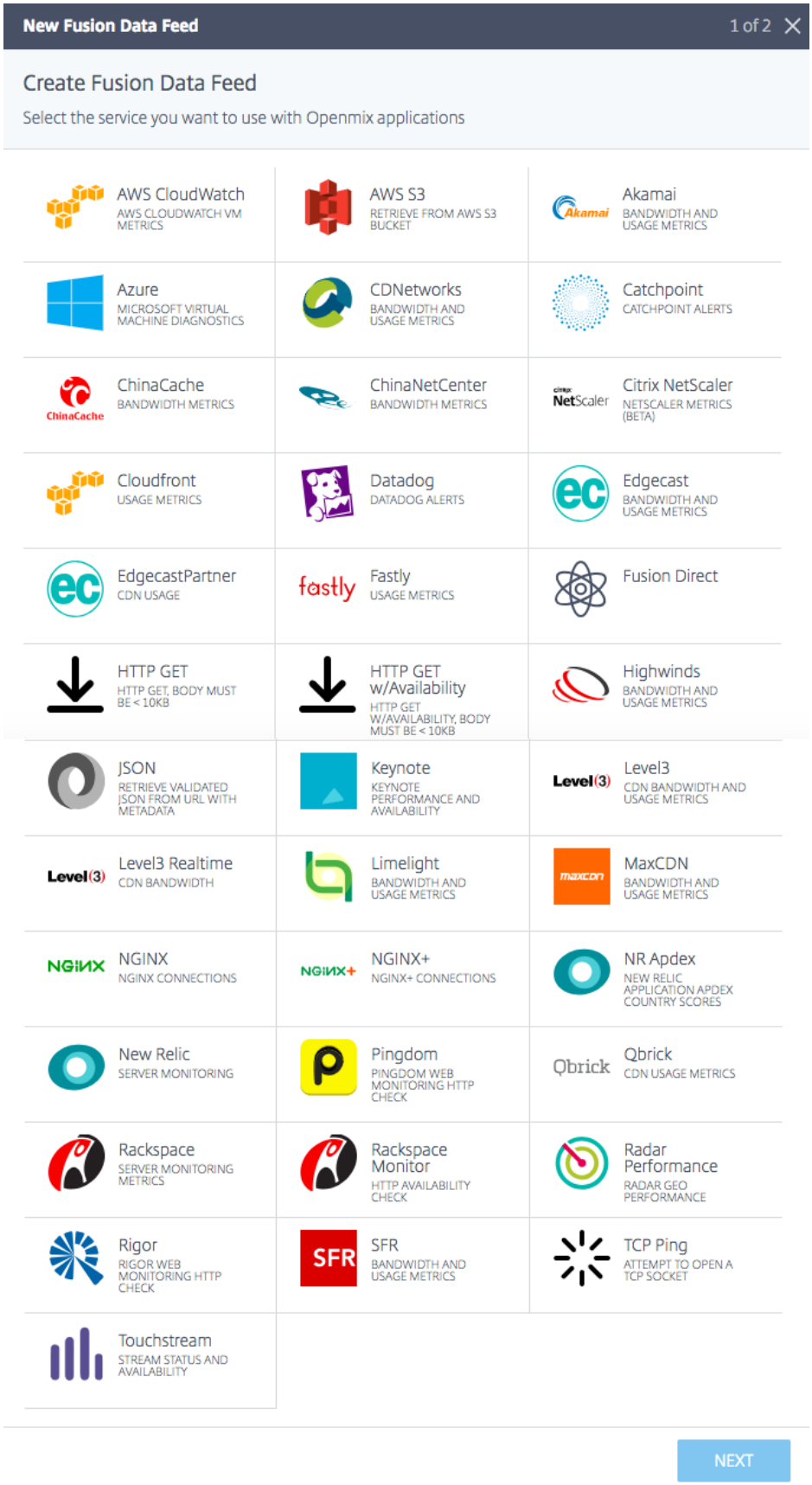


Haga clic en el botón **Comenzar** o en **+** para configurar una nueva fuente de datos.

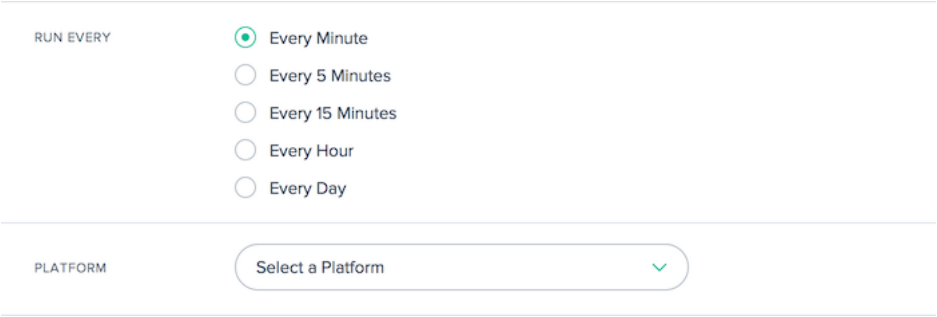


Nuevas fuentes de datos

Haga clic en el icono del servicio que desea integrar y rellene los campos de configuración requeridos.



Cada servicio requiere diferentes parámetros de configuración. Necesita un nombre de usuario y una contraseña o un token generado para la autenticación y cualquier configuración adicional específica del servicio.



Todas las fuentes de datos de Fusion están asociadas a una plataforma que se creó previamente en el portal NetScaler Intelligent Traffic Management. Esto permite a la aplicación Openmix en consulta los datos externos de Fusion para cada plataforma y, en función de la lógica de enrutamiento, determinar si la plataforma debe considerarse disponible para una decisión de enrutamiento.

La mayoría de las fuentes necesitan configurar los siguientes valores:

Elemento de entrada	Descripción
Ejecutar cada	Con qué frecuencia se actualiza la fuente de datos desde el servicio externo. Fusion llama al servicio en el intervalo especificado y actualiza las aplicaciones Openmix basándose en los nuevos datos.
Plataforma	La plataforma asociada a los datos Fusion en la aplicación Openmix.

Edición de fuentes de datos

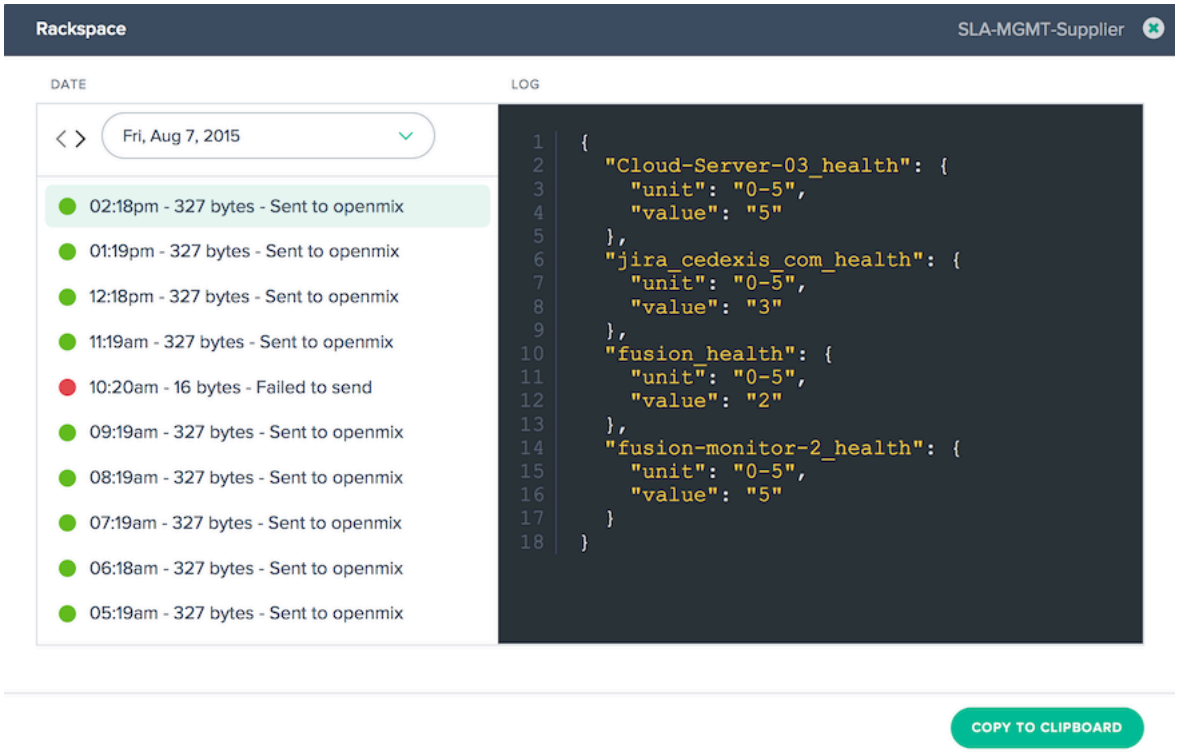
Modificar una fuente de datos de Fusion es tan fácil como hacer clic en la fuente de datos de la tabla y hacer clic en el botón **Modificar**.

Una vez que haya cambiado la configuración, haga clic en **Guardar**. Esto le devuelve a la lista de fuentes de datos con los cambios guardados y aplicados en la fuente de datos.

Historial de fuentes de datos

Fusion recopila las últimas 100 respuestas de cada vez que se ejecuta en el historial de fuentes de datos. Puede ver el estado de la fuente de datos, la información sobre los datos y la carga útil devuelta

por el servicio. Después de seleccionar la fuente de datos específica en la lista, haga clic en el botón **Historial de registro** en mostrar el historial de la fuente de datos.



Para cambiar la fecha seleccionada, puede hacer clic en los botones **<** o **>** para retroceder o avanzar desde la fecha seleccionada actual o elegir una fecha específica de la lista. Seleccione la marca de tiempo de la instancia específica y se mostrarán los datos devueltos por el servicio.

Fuentes de datos con errores

Cuarentena de Fusion para fuentes
de Fusion fallidas La cuarentena de Fusion se aplica en el feed de datos de Fusion defectuoso de un cliente, si el feed está configurado en ejecución en un intervalo de sondeo inferior a 24 horas. Fusion aplica la lógica de cuarentena para detener la ejecución de estas fuentes que fallan. Esto se hace en guardar recursos (CPU/memoria) y evitar cualquier impacto negativo en otros feeds de datos válidos de Fusion.

La lógica de cuarentena se aplica mediante la "copia de seguridad"de la alimentación de Fusion fallida a intervalos graduales. Esto ocurre hasta que el feed de Fusion se pone en cuarentena durante 24 horas. En este punto, el feed Fusion intentará correr cada 24 horas. La fuente de datos de Fusion que falla nunca se cierra por completo. Continuará en carrera, como mínimo dos veces cada 24 horas.

Importante:

- La fuente de datos Fusion siempre se ejecutará al menos dos veces consecutivas y fallará dos

veces antes de entrar en la lógica de cuarentena. Por ejemplo, si se ejecuta una alimentación de un minuto y falla dos veces consecutivamente, entrará en la lógica de cuarentena.

- Si en algún momento la fuente de datos de Fusion se ejecuta correctamente, se elimina de la lógica de cuarentena y se ejecutará de nuevo en su intervalo programado regularmente.
- Si en algún momento se actualiza la fuente Fusion (es decir, si el usuario ha introducido una URL incorrecta y la ha corregido, la fuente Fusion intentará ejecutarse de nuevo en un minuto, independientemente del intervalo de sondeo. Si tiene éxito, se eliminará de la lógica de cuarentena. Si continúa fallando, se aplicará la lógica de cuarentena.

Depuración global de CDN

June 4, 2021

La depuración global de CDN es una forma de purgar datos de varios CDN al mismo tiempo, lo que facilita la administración de varios CDN. Permite conectar los CDN que se van a depurar, especificar los URI que se van a depurar en todos los servicios adjuntos y hacer clic en el botón **Purgar**. La depuración se inicia en todos los CDN conectados.

La funcionalidad de depuración de CDN global se basa en tres componentes principales:

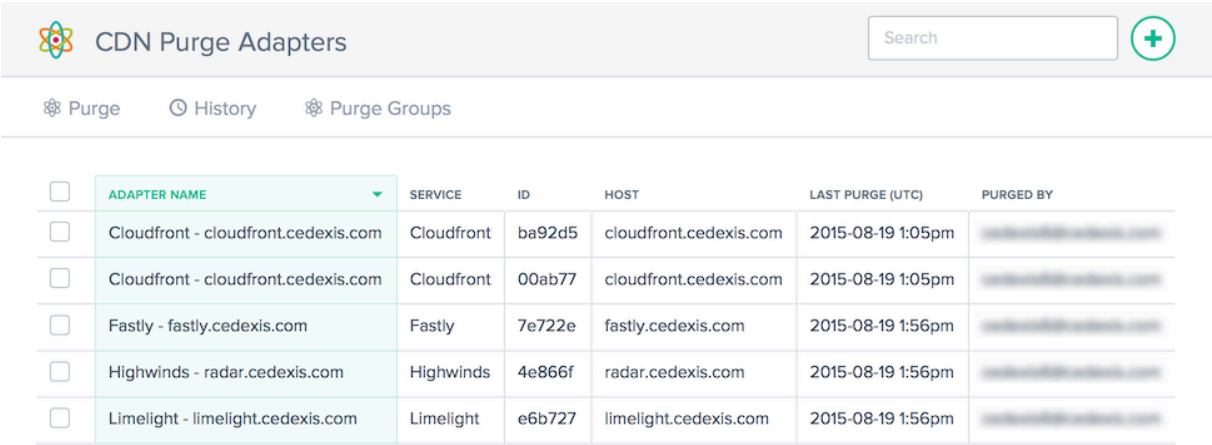
1. **Adaptador de purga de CDN**: Es necesario crear un adaptador de purga de CDN para cada combinación de nombres de CDN/host que desee depurar. El adaptador de purga de CDN recopila la información necesaria para ejecutar purgas, como: selección de servicios, información de autenticación, nombre de host y otra información específica del servicio. Necesita un adaptador de purga de CDN para cada nombre de host que se va a depurar en un CDN.
2. **URI**: Las purgas se ejecutan en una ubicación específica en los CDN.
3. **Grupo de depuración**: Los grupos de depuración permiten crear una colección lógica de adaptadores de purga de CDN y URI que se purgan con un comando. Por ejemplo, puede purgar el directorio '/media'en 2 CDN diferentes o un directorio que exista en el entorno de desarrollo, prueba y producción.

Los adaptadores de purga de CDN deben configurarse para ejecutar purgas. Los URI y varias purgas de CDN se pueden especificar individualmente, pero se recomienda que los grupos de purga de configuración administren purgaciones comunes que se ejecutan con frecuencia.

Se puede acceder a la Depuración de CDN global desde el nivel superior del menú de navegación como Depuración de CDN.

Adaptadores de purga de CDN

La siguiente pantalla muestra todos los adaptadores de purga de CDN configurados. La lista proporciona una visión general de los adaptadores CDN configurados y permite la ejecución de purga.



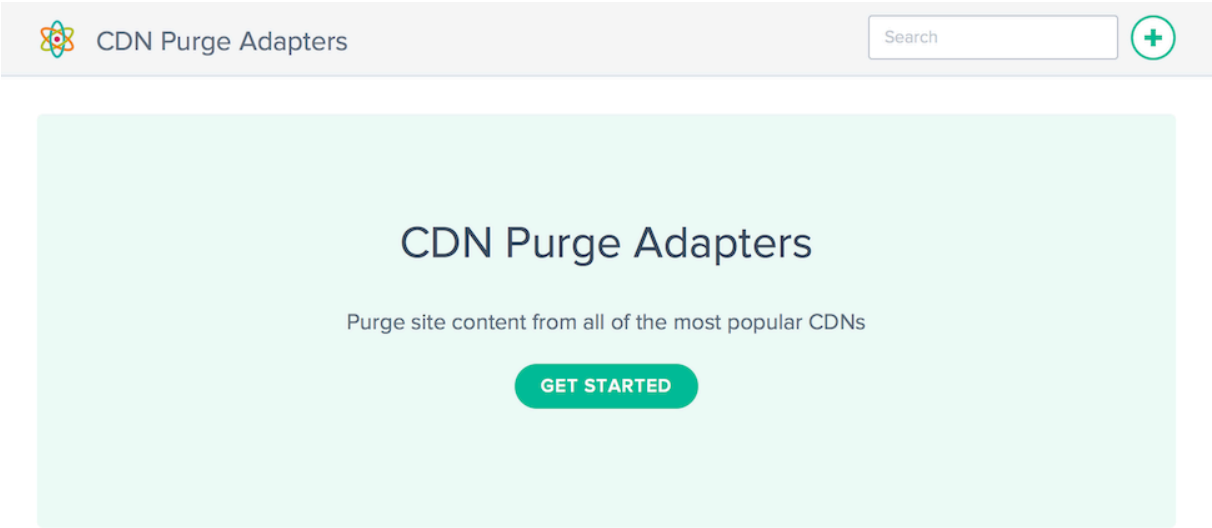
Las columnas proporcionan la siguiente información:

Se dirige	Descripción
Nombre del adaptador	Nombre dado al adaptador. Opcional, el valor predeterminado será “Servicio - Host”si no se especifica.
Servicio	El nombre del servicio CDN para el que se ha configurado la depuración.
IDENTIFICACIÓN	El ID del adaptador CDN. Esto es necesario para acceder a Fusion a través de la API.
Host	Host con el que está configurada la depuración para ejecutarse. Los servicios a veces llaman a esta configuración: host, nombre de host, plataforma, etc.
Última depuración (UTC)	Hora y fecha, en UTC, en la que se ejecutó la depuración por última vez.
Depurado por	El usuario que ejecutó una depuración por última vez.

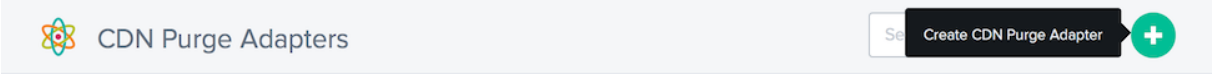
Creación de adaptadores de depuración de CDN

Para utilizar la depuración global de CDN, debe agregar las configuraciones de CDN y nombre de host. Cuando abra por primera vez **Depuración de CDN**, se le pedirá que cree un adaptador de purga de

CDN.

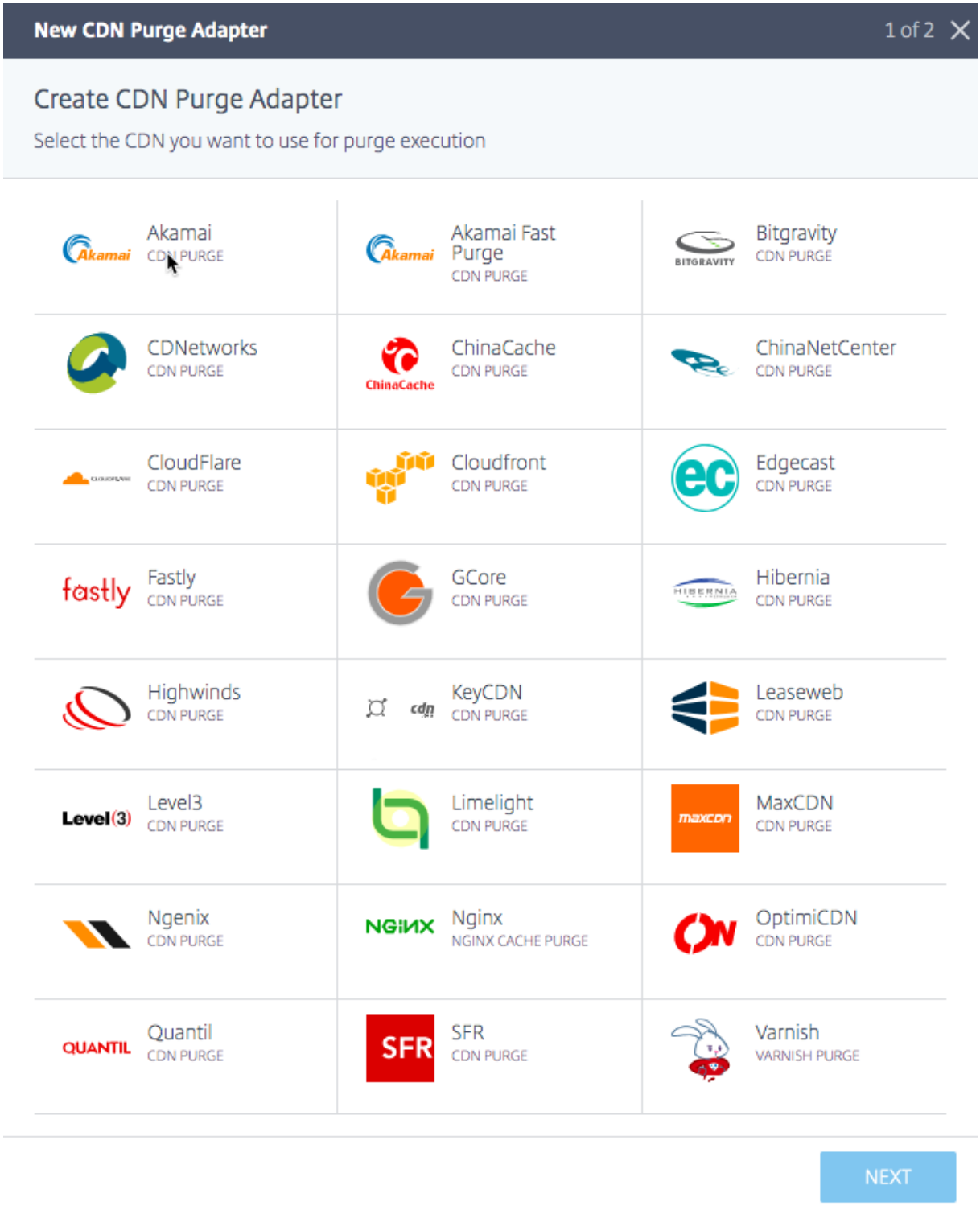


Haga clic en el botón **Empezar** o **+** para configurar una CDN disponible para depurar.

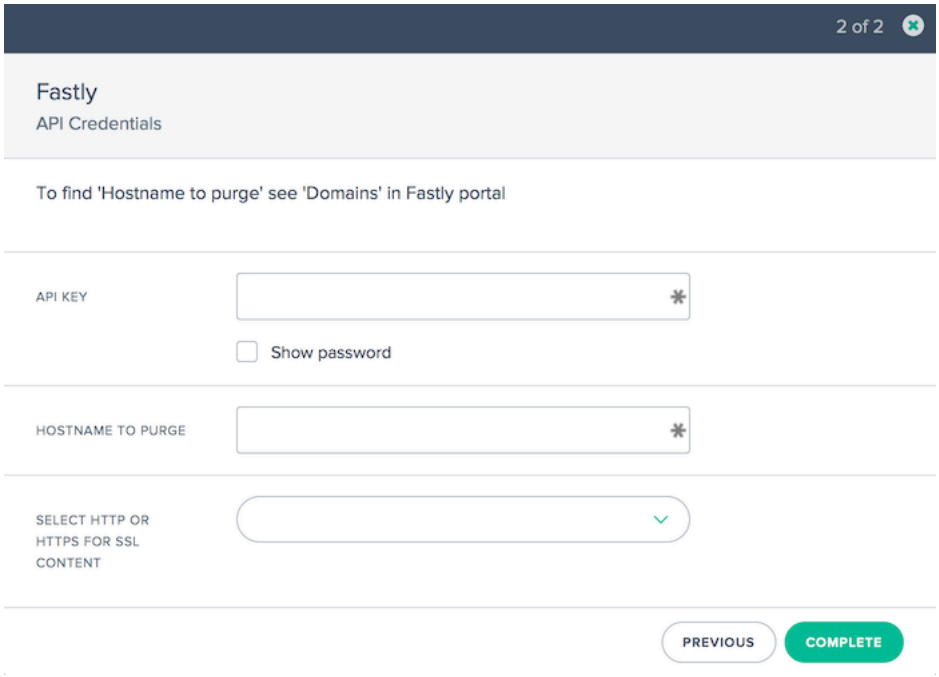


Nuevos adaptadores de purga de CDN

Haga clic en el icono del servicio para el que desea crear un adaptador de purga de CDN y rellene los campos de configuración necesarios.



Cada adaptador de purga requiere diferentes parámetros de configuración. Necesitaría un nombre de usuario y una contraseña o un token generado para la autenticación y cualquier configuración adicional específica del servicio.



Edición de adaptadores de purga de CDN

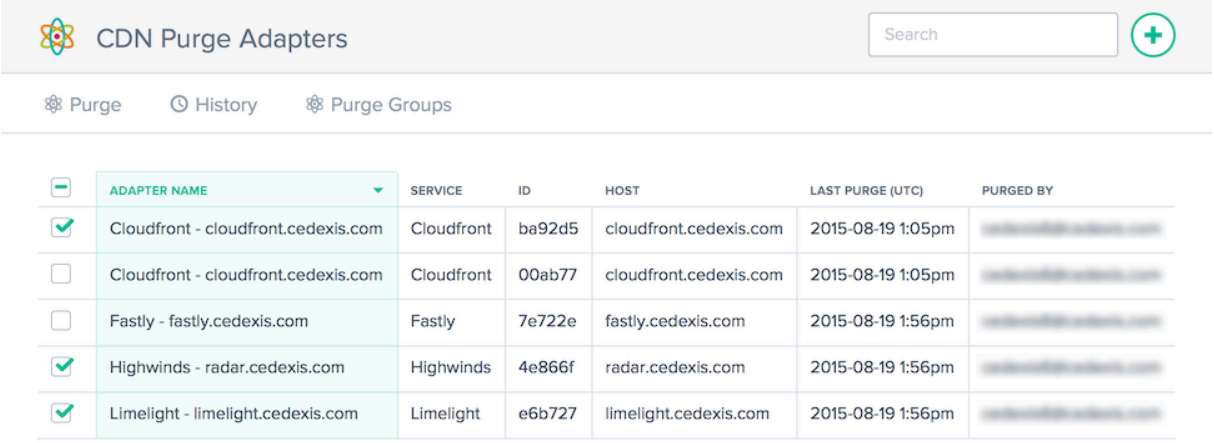
Modificar un adaptador de purga de CDN es tan sencillo como hacer clic en el adaptador de purga de CDN en la tabla y hacer clic en el botón **Modificar**.

Una vez que haya cambiado la configuración, haga clic en **Guardar**. De este modo, volverá a la lista de adaptadores de purga con los cambios guardados y aplicados al adaptador de purga de CDN específico.

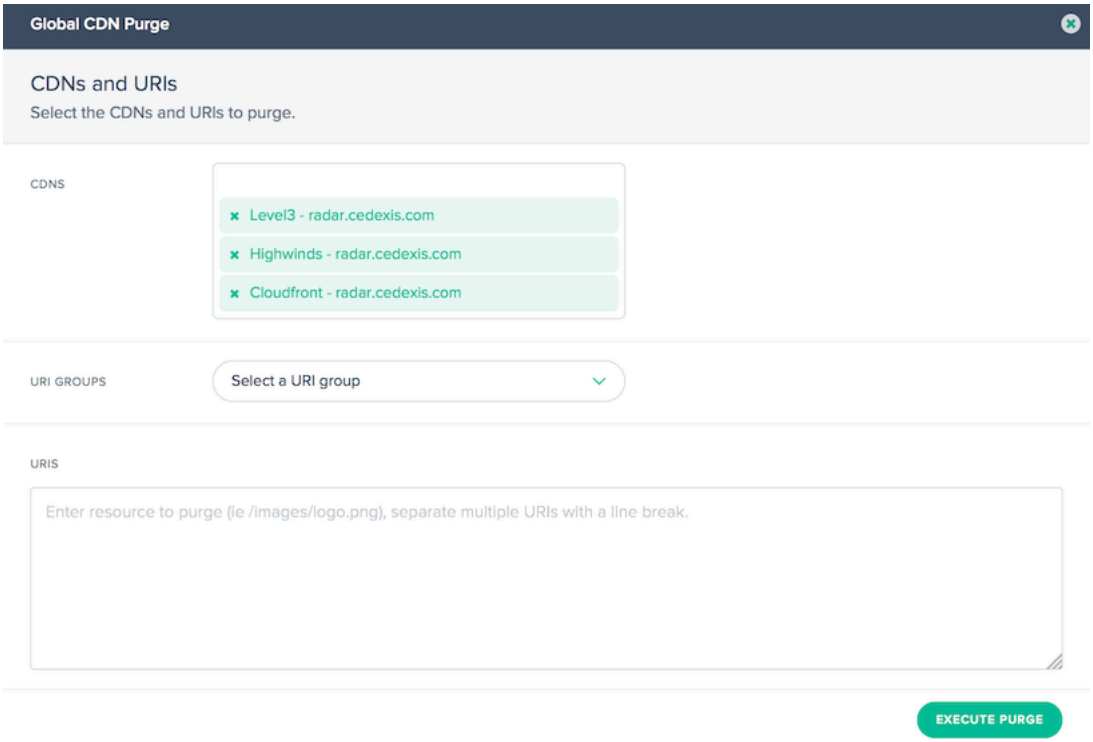
Ejecución de una Depuración

Para ejecutar una depuración, seleccione los adaptadores de purga de CDN que deben incluirse en la ejecución de purga.

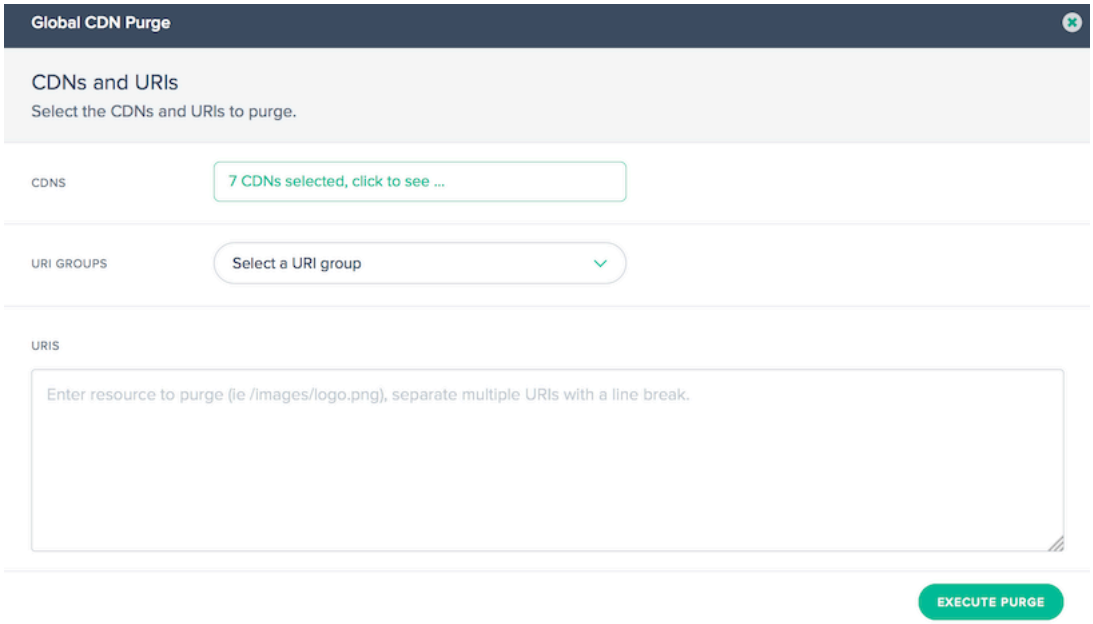
Haga clic en el botón **Depurar** para iniciar el proceso de depuración.



Se abrirá el cuadro de diálogo **Depuración global de CDN**. El cuadro de diálogo muestra los adaptadores de purga de CDN que se seleccionaron y los URI que se utilizan en la ejecución de purga.

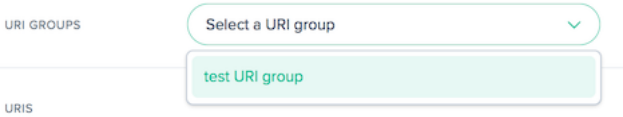


Si hay 5 adaptadores de purga CDN seleccionados o menos, el cuadro de diálogo de purga muestra la lista completa de los adaptadores de purga CDN seleccionados. Si no se muestran todos los adaptadores de depuración de CDN, haga clic en el cuadro de texto **CDN** que dice **X CDN seleccionados, haga clic para ver…** para mostrar todos los adaptadores de depuración seleccionados.

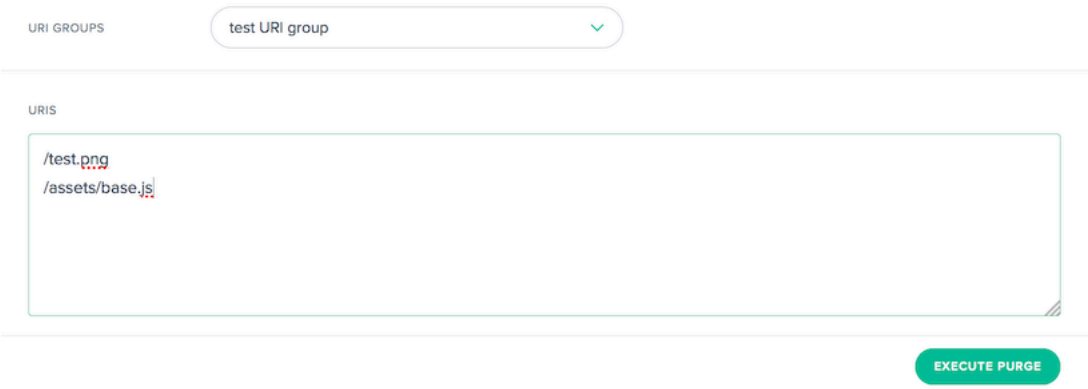


La lista se puede ocultar haciendo clic en el botón **Ocultar** situado a la derecha de la lista de adaptadores de purga.

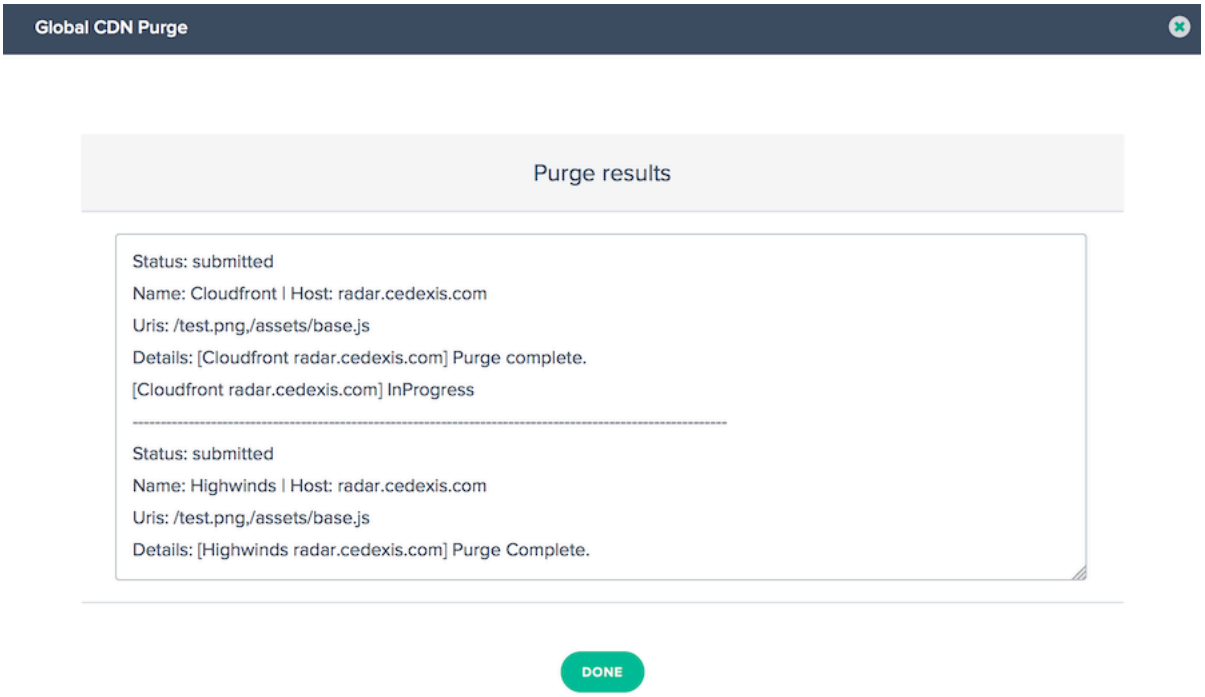
Puede rellenar los URI utilizados en la depuración introduciendo manualmente los URI o seleccionando entre los Grupos URI disponibles. Al seleccionar un grupo de URI, se rellena la entrada de URI con los URI del grupo de depuración seleccionado.



Introduzca o modifique los URI de los recursos que se deben depurar.

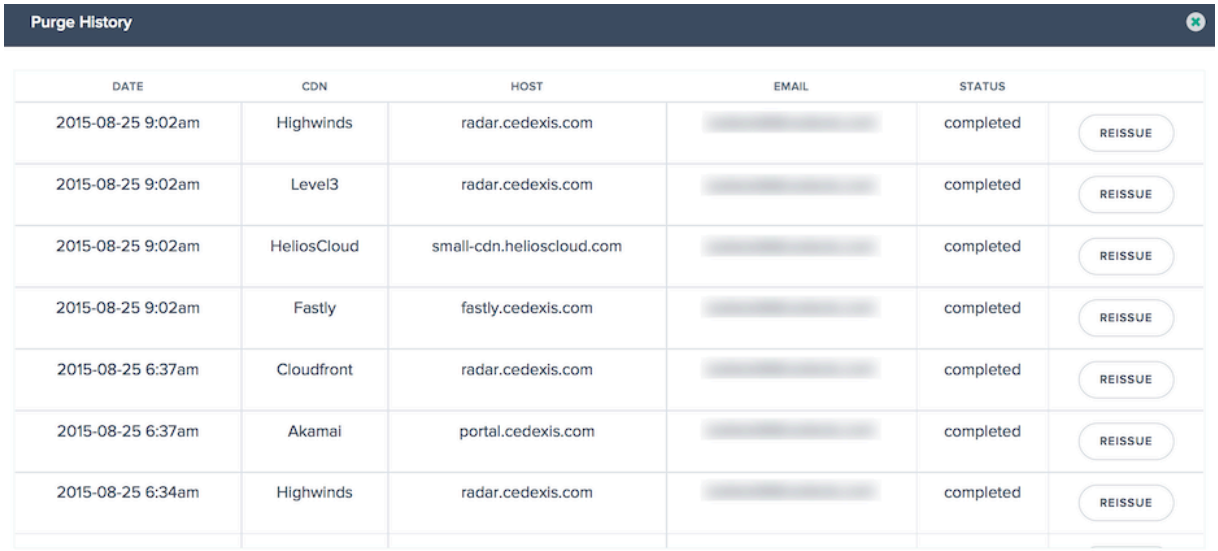


Cuando esté listo para ejecutar la solicitud de depuración, haga clic en el botón **Ejecutar depuración**. La depuración se envía a todos los CDN seleccionados. Los envíos y las respuestas de API se muestran en el cuadro de diálogo **Depurar resultados**.

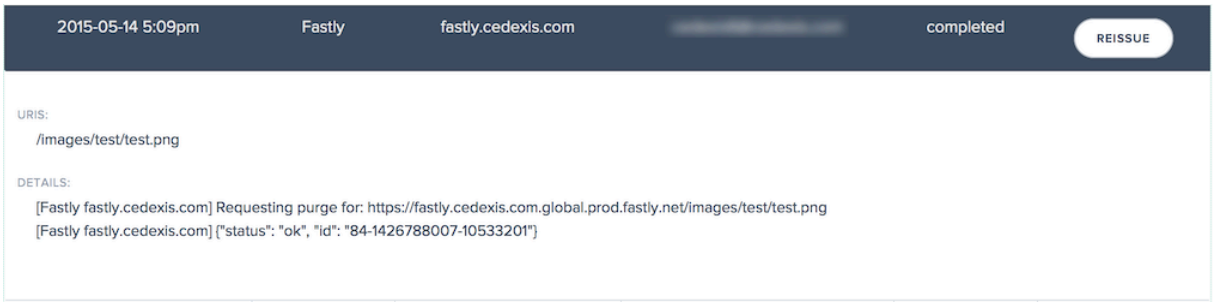


Historial del adaptador de purga de CDN

Fusion recopila el historial de purga cada vez que se ejecuta. Puede ver el estado de depuración, la información sobre la depuración y los mensajes devueltos por el servicio. Para ver el historial de depuración, haga clic en el botón **Historial** de las pantallas **Adaptadores de depuración de CDN o Grupos de depuración**.



La lista incluye la hora y el estado de las últimas 100 ejecuciones de purga. Puede ver los detalles de una solicitud de depuración enviada al servicio CDN haciendo clic en la fila deseada de la tabla. La información detallada incluye los URI especificados para la depuración y las respuestas de API devueltas por el servicio durante la depuración.



Si desea volver a ejecutar una depuración específica que contiene el historial, haga clic en el botón **Reemitir** a la derecha de la información de estado de depuración. El cuadro de diálogo de depuración aparece con los datos de la depuración anterior precargados para ejecutarse.

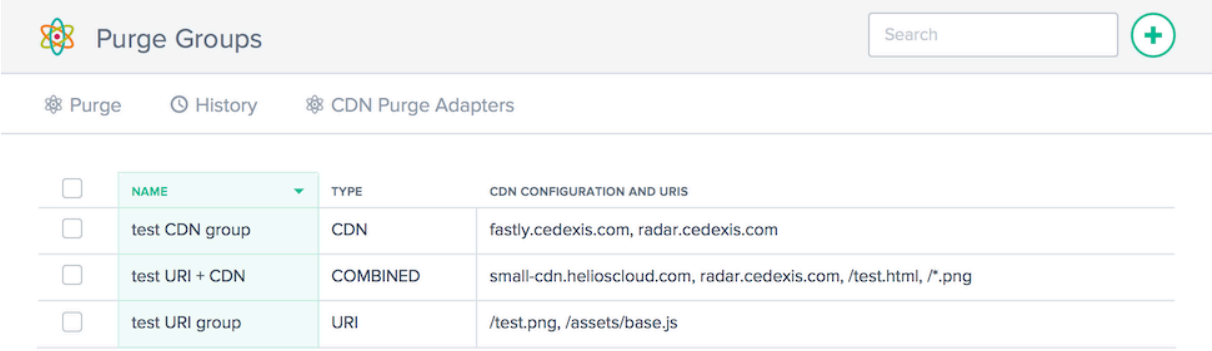
Grupos de Depuración

Los grupos de depuración permiten organizar adaptadores de purga de CDN y URI para facilitar la depuración de un conjunto lógico de recursos. Por ejemplo, es posible que desee agrupar entornos de desarrollo, prueba y producción y depurarlos todos al mismo tiempo. O purgue todos los recursos de imagen en varios CDN a la vez.

Los grupos de depuración pueden estar formados por una colección de adaptadores de purga CDN, URI de purga o ambos. Normalmente, un grupo que contiene solo adaptadores de purga de CDN se utiliza para purgar diferentes recursos en varios servicios. Un grupo combinado se utiliza a menudo

para especificar previamente una purga estándar y reutilizable, como “todos los medios en todos mis sitios web regionales y CDN”.

Cuando tenga al menos una configuración de grupo de depuración, verá esta pantalla al abrir Depuración de CDN.



Las columnas proporcionan la siguiente información:

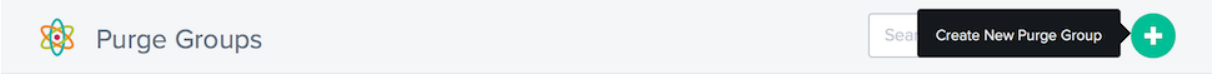
Se dirige	Descripción
Nombre	Nombre del grupo de depuración.
Tipo	El tipo de contenido del grupo. + CDN: el grupo de depuración contiene sólo adaptadores de depuración de CDN y el usuario necesita especificar URI al ejecutar el URI de depuración + —el grupo de depuración contiene sólo URI y el usuario tendrá que especificar servicios al ejecutar la depuración + Combinado: el grupo de depuración contiene ambos CDN los adaptadores de purga y los URI; el usuario podrá ejecutar la depuración sin necesidad de especificar más información
Configuración de CDN y URI	Los adaptadores y/o URI de purga de CDN incluidos en la definición de grupo.

Creación de Grupos de Depuración

Para utilizar grupos de depuración, debe especificar los adaptadores de purga de CDN o URI que deben incluirse. Existen dos formas de crear grupos:

En la página Adaptadores de depuración de CDN, puede comprobar los adaptadores de depuración deseados y, a continuación, hacer clic en **Crear grupo de depuración**.

En la página Depurar grupos, haga clic en **+** para crear un grupo.

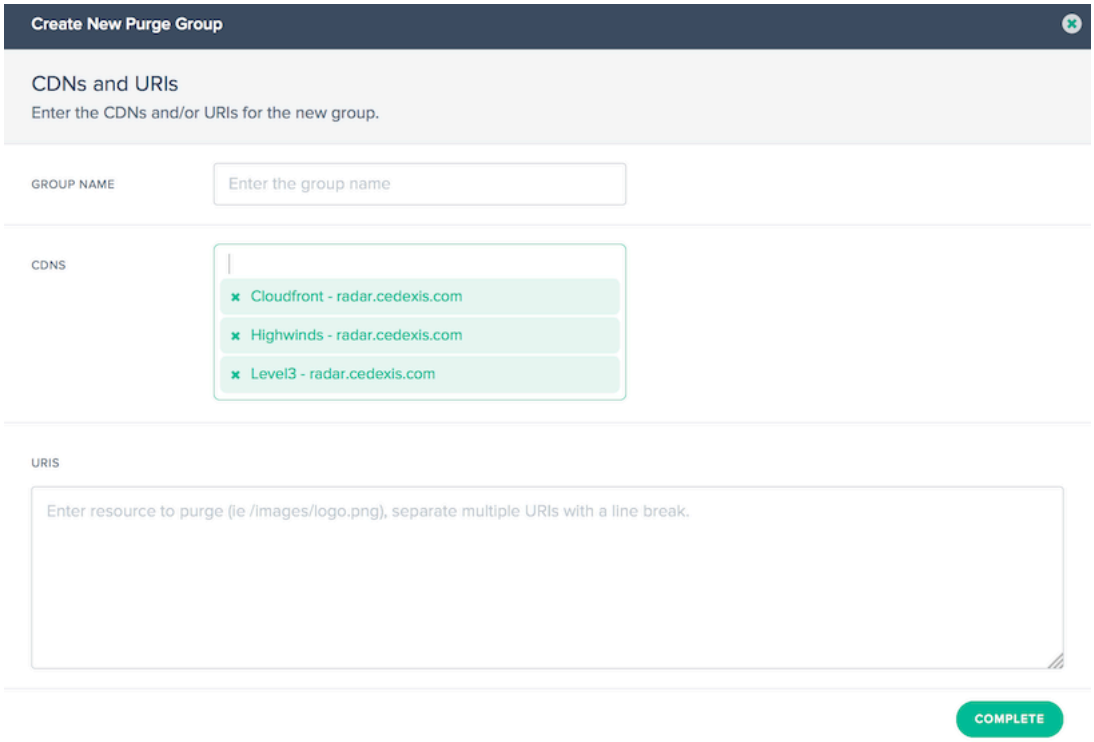


En ambos casos, se muestra el cuadro de diálogo **Crear nuevo grupo**.

Introduzca el nombre del grupo de depuración.

> **NOTA:** Puede agregar o quitar adaptadores de purga de CDN de la lista.

Haga clic en **Completar** para crear el grupo.



Ejecución de una Depuración de Grupo

En la página Grupo de Depuración, seleccione uno o varios grupos y, a continuación, haga clic en el botón **Depurar**. Se abrirá el cuadro de diálogo **Depuración de CDN** con los parámetros especificados por la definición de grupo de depuración.

Haga clic en el botón **Ejecutar depuración**para iniciar la depuración configurada.

Alertas

September 13, 2023

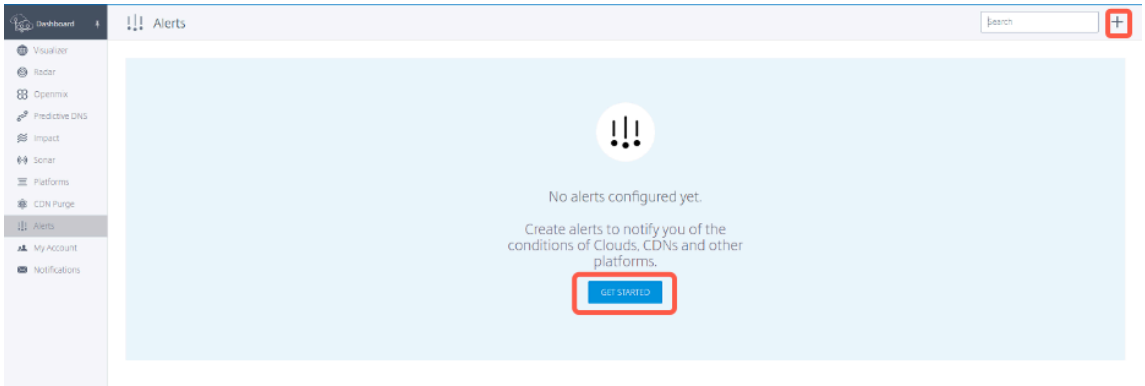
La función **Alertas** supervisa los problemas o anomalías de rendimiento de las plataformas configuradas desde una red de usuarios finales en todo el mundo.

Crear alertas

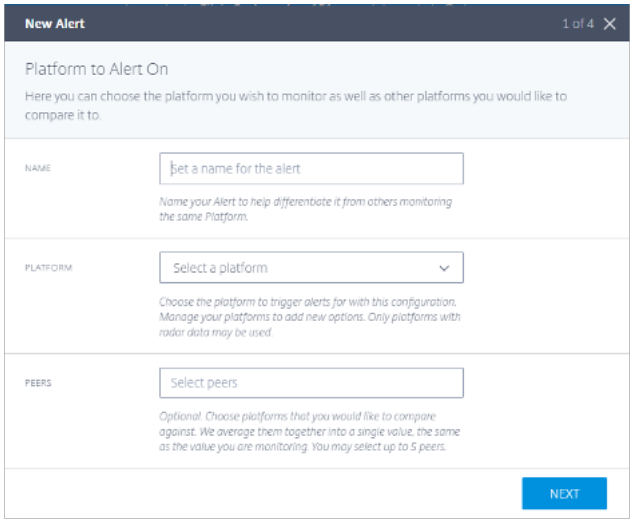
Para crear alertas que supervisen el rendimiento de sus plataformas, primero tiene que configurar sus plataformas. En la barra lateral izquierda, haga clic en **Plataformas** para ir a la pantalla de la plataforma y configurar sus plataformas.

Para agregar una alerta nueva:

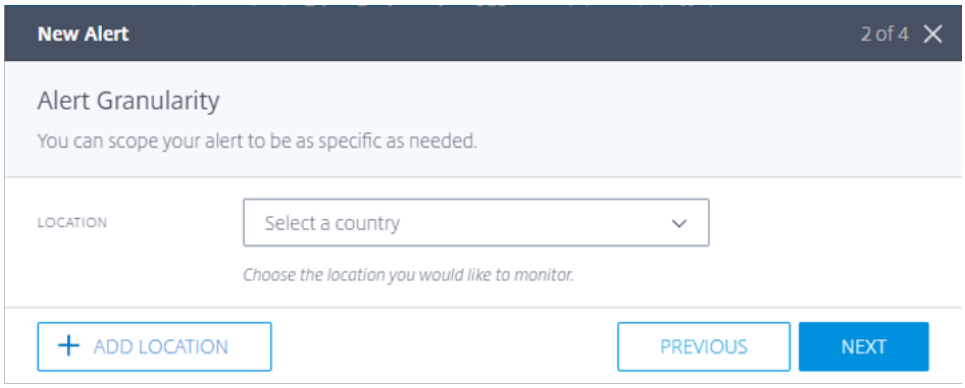
1. En la barra lateral izquierda, haga clic en **Alertas** para ir a la página de alertas y crear alertas.
2. En la página de alertas, haga clic en **EMPEZAR** o en el símbolo **+** de la esquina superior derecha.



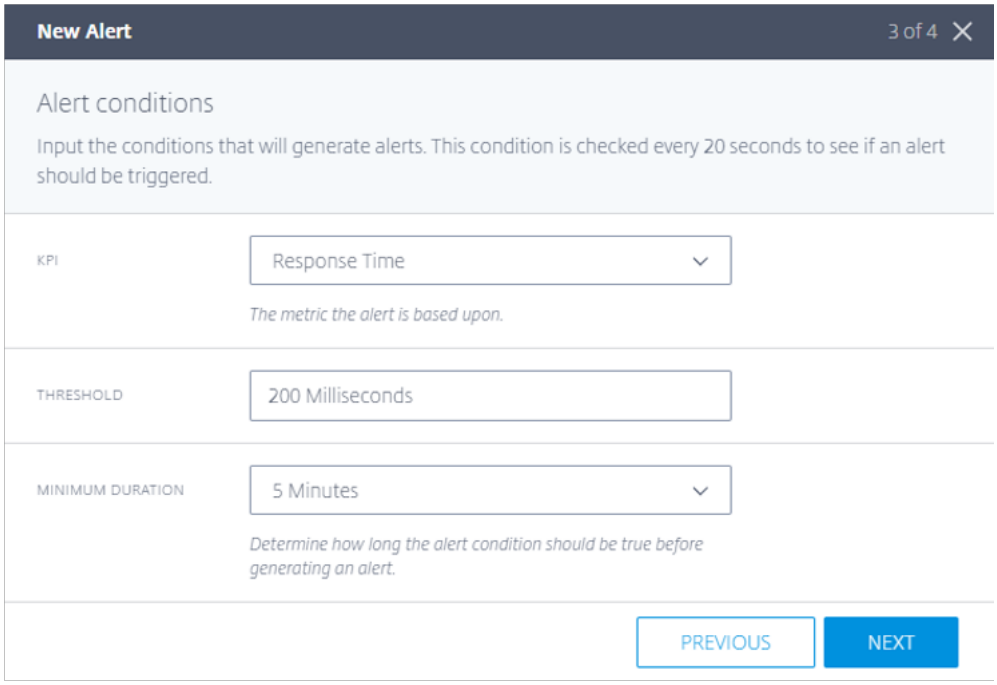
3. En la ventana **Nueva alerta** :
   - introduzca el nombre de la alerta
   - seleccionar la plataforma relativa que se va a monitorizar
   - seleccionar plataformas de pares para compararlas (puede seleccionar hasta 5 pares). Este parámetro es opcional.
   - haga clic en **Siguiente**.



4. Seleccione la **ubicación** y la **red** para las que quiere supervisar las alertas y haga clic en **Siguiente**.



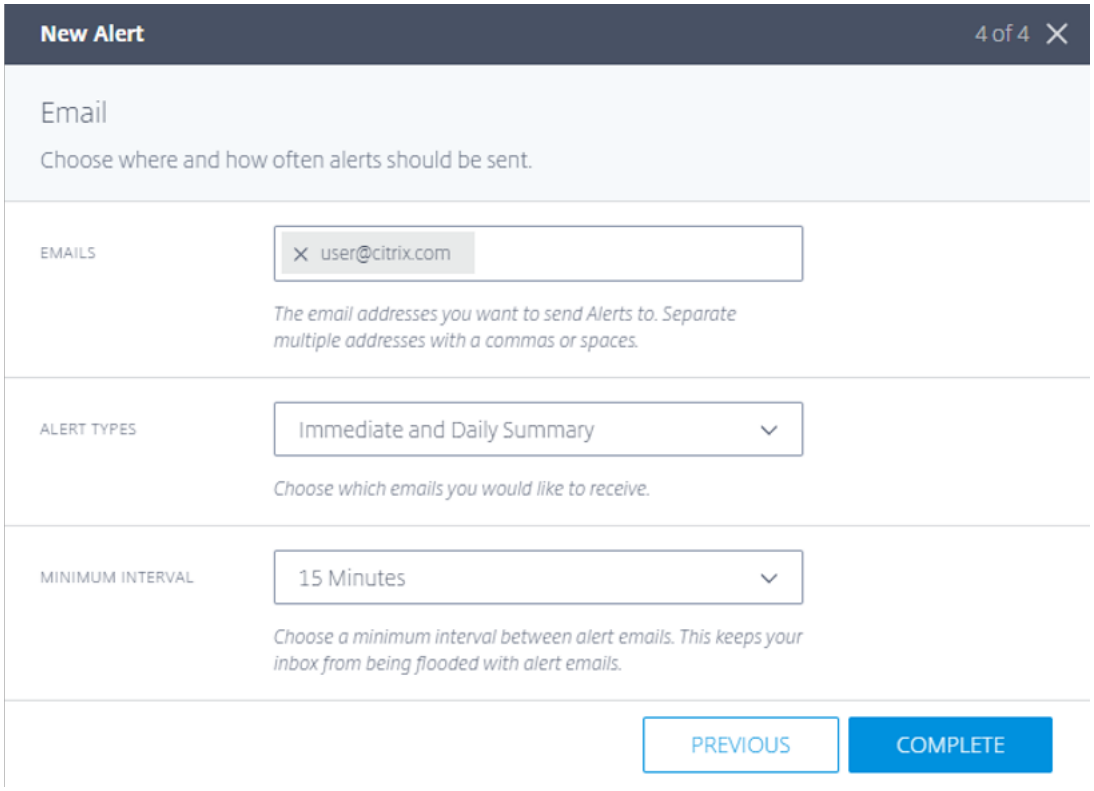
5. Seleccione el **KPI**, el **umbral**y la **duración mínima** del evento que desencadena la alerta.



NetScaler Intelligent Traffic Management proporciona los siguientes KPI:

- **Tiempo de respuesta:** el valor del umbral indica el valor máximo (en milisegundos) aceptado antes de que se active la alerta. Para que se active una alerta, la medición debe ser mayor que el umbral durante al menos el **tiempo ≥ minimum_duration** que el usuario seleccionó. La misma alerta se activará después de recibir una medición por debajo del umbral nuevamente durante al menos un tiempo ≥ duración mínima.
- **Disponibilidad:** el valor del umbral indica el valor mínimo aceptado antes de que se active la alerta. Para que se active una alerta, la medición debe ser inferior al umbral durante al menos el **tiempo ≥ minimum_duration** que el usuario seleccionó. La misma alerta se activará después de recibir una medición por encima del umbral nuevamente durante al menos un tiempo mayor o igual a ≥ duración mínima.
- **Rendimiento:** el valor del umbral indica el valor mínimo (en kbps) aceptado antes de que se active la alerta. Para que se active una alerta, la medición debe ser inferior al umbral durante al menos el **tiempo ≥ minimum_duration** que el usuario seleccionó. La misma alerta se activará después de recibir una medición por encima del umbral nuevamente durante al menos un tiempo mayor o igual a ≥ duración mínima.

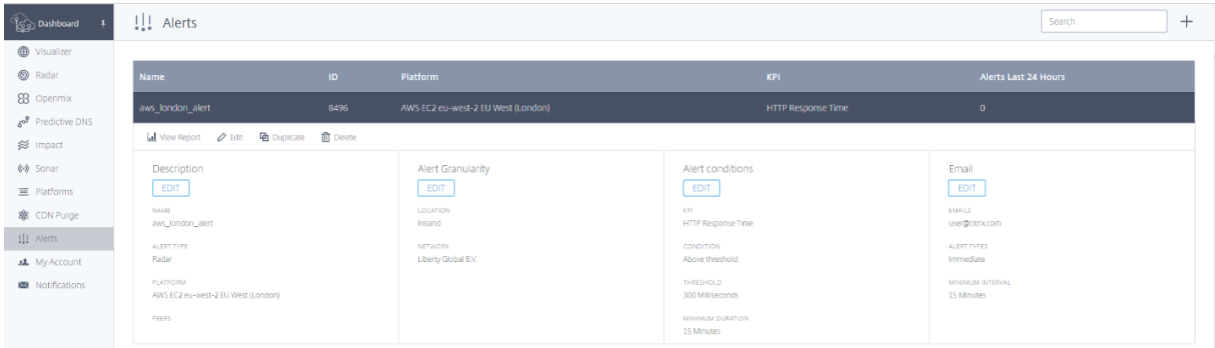
6. Introduzca las direcciones de correo electrónico a las que quiere enviar alertas, seleccione el tipo de alerta y seleccione el intervalo mínimo entre los correos electrónicos de alertas.



Los tipos de alertas son los siguientes:

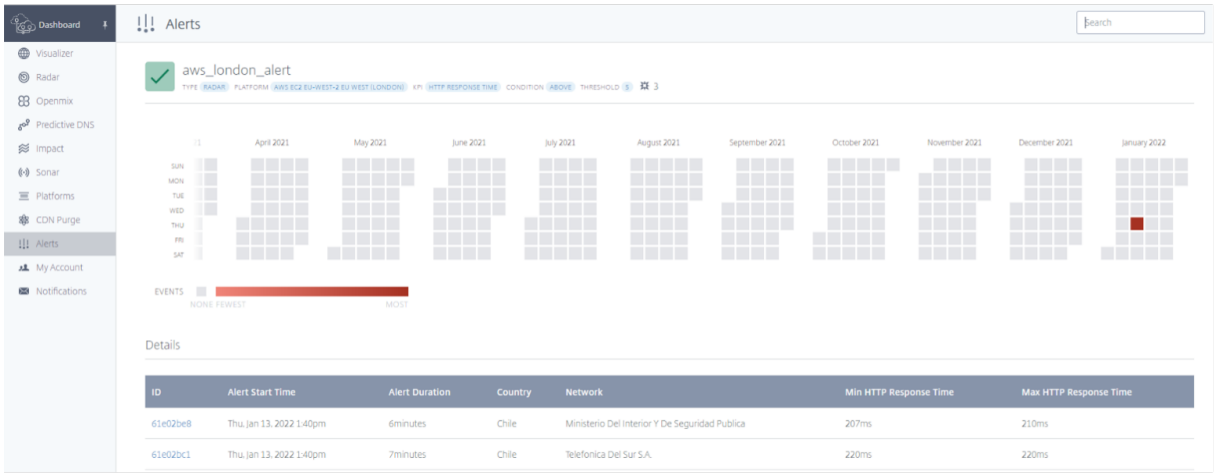
- **Inmediato:** esta opción envía un correo electrónico inmediatamente cuando se activa una alerta.
- **Resumen diario:** esta opción solo envía un correo electrónico cada medianoche en hora universal coordinada (UTC), incluidos todos los eventos que se activan.
- **Resumen inmediato y diario:** esta opción es una combinación de envío de correo electrónico inmediato y diario.

7. Después de configurar una alerta, puede ver las alertas en la ficha **Alertas** y el mapa global en la ficha **Visualizador**. Para ver el informe de una alerta específica, haga clic en **Ver informe** en la ficha **Alertas**.



La siguiente página de informes muestra los eventos que se supervisan cada día durante todos los

meses. Por ejemplo, en la siguiente captura de pantalla, hay 3 incidentes supervisados el mismo día de enero de 2022.



Puede hacer clic en cualquier incidente o evento específico para ver los detalles, como se muestra en la siguiente imagen:

Supervisión de la experiencia de red

September 13, 2023

Introducción

El servicio**Citrix Network Experience Monitoring (NEM)** (anteriormente denominado **Netscope**) permite a los proveedores de servicios, empresas, ISP y proveedores de servicios de terceros acceder

a registros detallados de medición de Radar e informes estándar en forma de datos resumidos accionables. NEM ofrece varios registros e informes estándar que los clientes pueden utilizar para medir la calidad de sus servicios.

Esta solución incluye la entrega de medición de radar "sin procesar"y el acceso a la API de datos de ITM de Citrix. NEM proporciona tanto los datos granulares (como mediciones brutas o agregados de datos) como las alertas de umbral de datos. Estos servicios ayudan con el descubrimiento, aíslan la disponibilidad de la plataforma y los problemas de rendimiento en los pares de plataforma y los ISP subyacentes.

Mediciones "brutas"de radar: las mediciones de radar proporcionan información granular por evento que se procesa en lotes a diario. Las mediciones de radar incluyen datos de medición públicos, comunitarios y privados recopilados por la etiqueta. Se incluyen datos como la disponibilidad, el tiempo de respuesta y el rendimiento de las mediciones HTTP y HTTPS. Se proporcionan los siguientes campos de datos:

- ID de proveedor, IP de resolución, IP de cliente ofuscadas (/28)
- Encabezado de referencia ofuscado, agente de usuario, ASN de usuario final
- Datos geográficos para campos de resolución y cliente

Las métricas de radar que están disponibles en las medidas "RAW"son:

- Disponibilidad, tiempo de respuesta y rendimiento (cuando se mide)
- Hora de búsqueda de DNS (opcional), hora de conexión TCP (opcional) y hora de conexión segura (opcional)
- Latencia (opcional)
- Tiempo de descarga (opcional)

Las mediciones de radar están disponibles para permitir a los clientes realizar sus propios análisis de los datos recopilados. El conjunto de datos incluye información sobre el rendimiento y la disponibilidad del proveedor (errores) para una serie de protocolos de comunicación.

Los datos de los archivos de registro están disponibles durante 7 días, desde un depósito de AWS S3 o Google Cloud Storage. Los clientes pueden recuperar archivos de registro de datos comunitarios y privados mediante métodos de acceso a depósitos estándar.

Medidas "RAW"de radar en tiempo real (opcional): Las mediciones Raw Radar se entregan en tiempo real a un bucket de AWS S3. Por lo general, estos registros están disponibles dentro de los 5 minutos posteriores a la recopilación Proporcionan tanta granularidad como las mediciones sin procesar de radar señaladas anteriormente.

API de datos: la API de datos de Radar ITM de Citrix proporciona agregados de datos de medición privados y de la comunidad pública de Radar. Los datos se actualizan continuamente y se almacenan por lotes aproximadamente cada 60 segundos para que la API los recupere. La API de datos se proporciona para permitir a los clientes integrar datos de Radar en sus propios informes y paneles.

Uso compartido y entrega de registros

- Los registros de Radar se pueden entregar en tiempo real y diariamente.
- Los informes se publican diariamente.
- Los resultados se guardan en AWS S3 (S3) o Google Cloud Storage (GCS).
- Tanto los registros como los informes tienen un período de retención de 7 días y se eliminan automáticamente una semana después de su creación.
- Los informes suelen estar en formato TSV (valores separados por tabulaciones) o JSON, según el tipo de informe.

Los clientes reciben información de inicio de sesión para acceder a los depósitos de S3 y GCS. Se puede usar una herramienta de línea de comandos como s3cmd o la CLI de AWS para S3 o gsutil para GCS para iniciar sesión. El archivo de configuración de S3cmd reconoce las claves de acceso recibidas a través de la interfaz de usuario del portal y ayuda al usuario a conectarse al bucket de S3.

La CLI de AWS debe instalarse en el equipo del cliente para conectarse a S3 y acceder a los registros. Para GCS, el cliente recibe el archivo de clave de acceso como una descarga a través de la interfaz de usuario del portal, que se puede usar con la herramienta gsutil. Para obtener más información, consulte las preguntas frecuentes.

Los clientes reciben notificaciones por correo electrónico cuando los informes están disponibles.

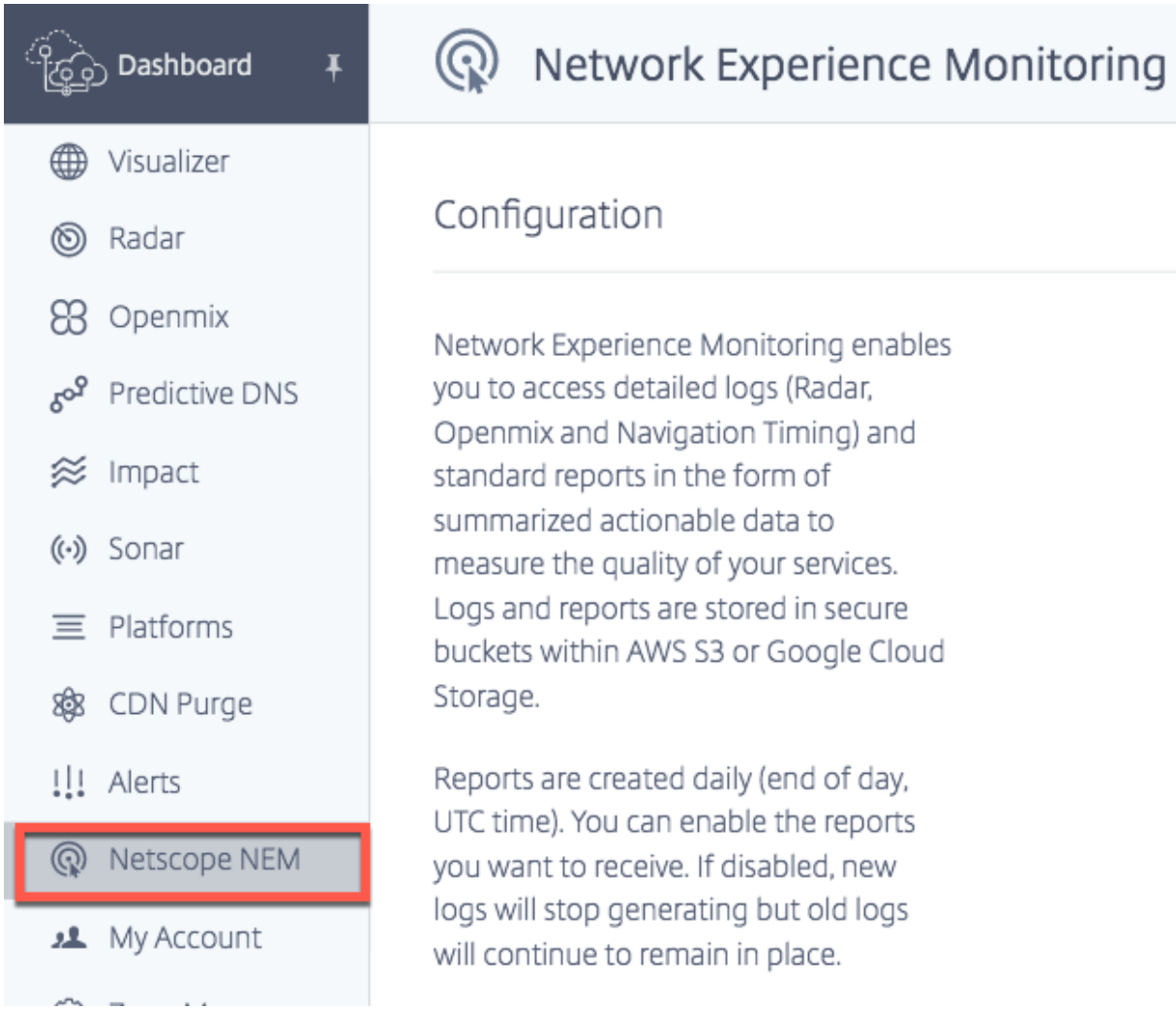
Configuración de la plataforma

Debe configurar su plataforma para admitir y producir los datos necesarios para Netscope NEM. Antes de empezar, asegúrese de que la siguiente configuración esté habilitada para su plataforma:

- Para los informes Best anónimos, habilite **Configuración de sondeo de Radar**.
  - Para el mejor RTT anónimo, habilite el **tiempo de respuesta y la disponibilidad**.
  - Para el mejor rendimiento anónimo, habilite **el rendimiento y la disponibilidad**.
- Para los informes de ID de nodo de caché, habilite **Configuración de sonda de Radar**y, en **Configuración avanzada de Radar**, habilite **ID de nodo**.
- Para Detalles de sincronización de recursos, habilite **Incluir marcas** de tiempo en **Configuración avanzada de Radar**.

Navegación

En el menú principal, seleccione **Netscope NEM**. Se abre la página **Network Experience Monitoring** Configuration.



Plataformas y Redes

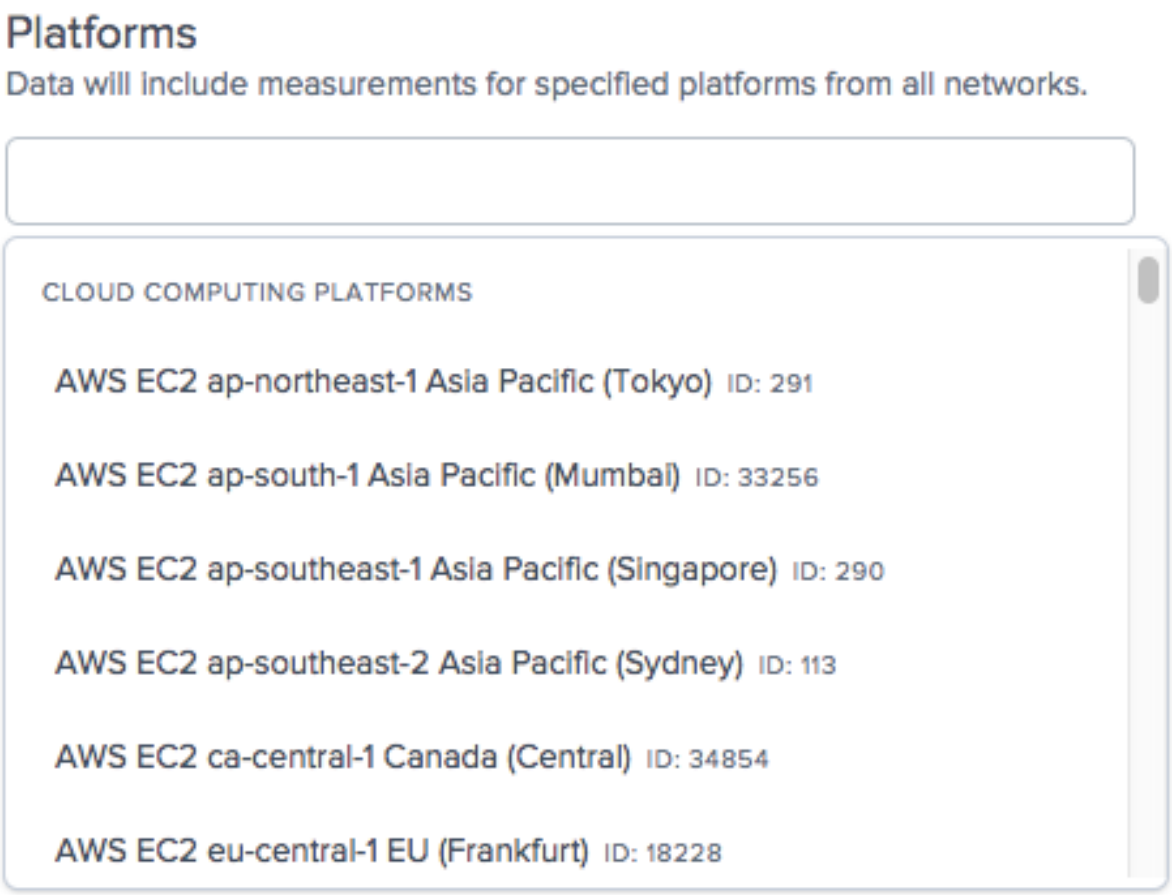
Seleccione **Plataformas** o **Redes** requeridas (o ambas) para iniciar el proceso de configuración.

> **NOTA:**
>
> Los registros e informes solo se pueden configurar y generar si se selecciona al menos una **plataforma** o **red**.

Los datos resumidos que recibe el cliente incluyen mediciones de radar de plataformas seleccionadas (para todas las redes asociadas) o redes seleccionadas (para todas las mediciones de plataforma asociadas).

Selección de plataformas

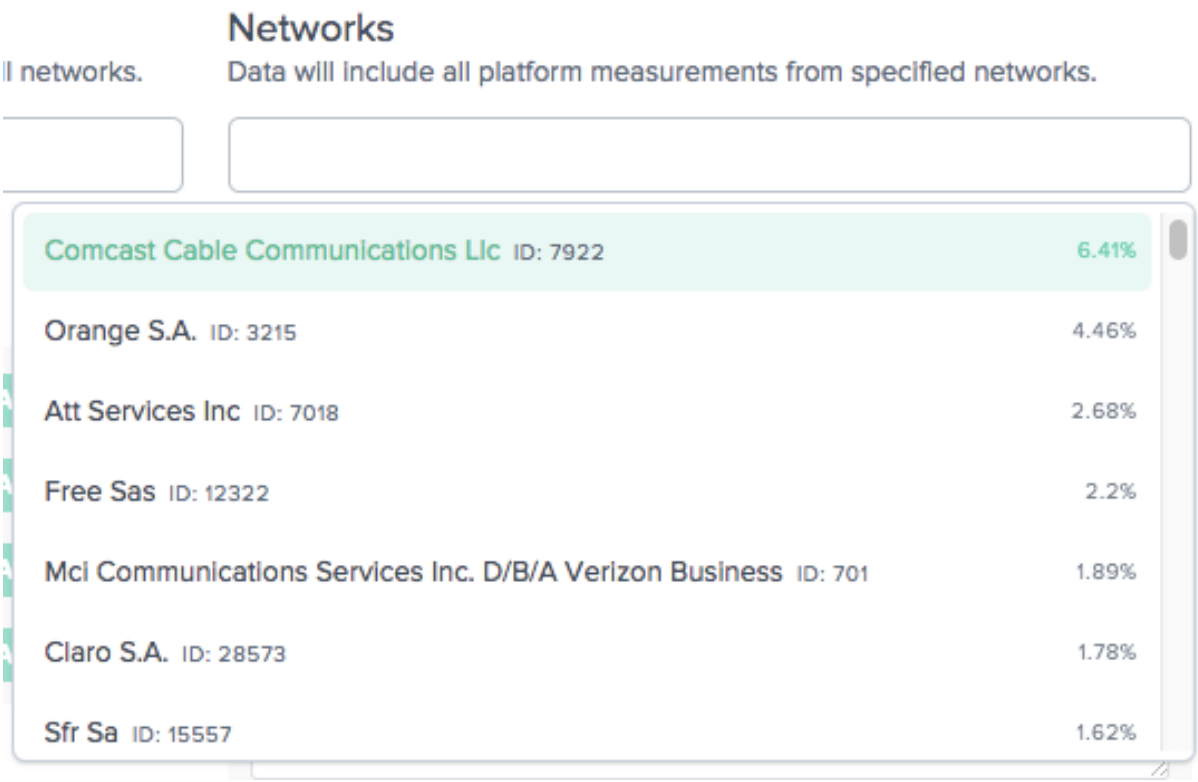
Para empresas o proveedores de servicios de contenido, seleccione plataformas como CDN, nubes, centros de datos u otros puntos finales. Seleccione las plataformas para las que se requieren mediciones.



Selección de redes

En el caso de los ISP, seleccione **las redes** de la lista asociada a diferentes plataformas o puntos finales para los que se requieren mediciones.

> **NOTA:**
>
> Si no encuentra la plataforma necesaria en la lista, puede configurarla en la sección **Plataforma** del portal. Para redes no disponibles, póngase en contacto con el equipo de asistencia.



Informes de plataforma

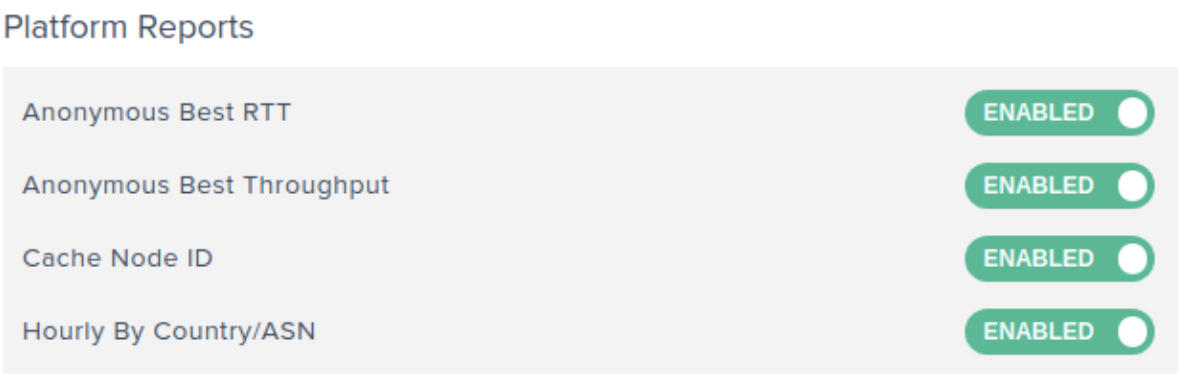
Existen cuatro tipos de **informes de plataforma**:

1. **Mejor anónimo para el tiempo de ida y vuelta (RTT)**
2. **Mejor anónimo para el rendimiento**
3. **ID de nodo de caché**
4. **Cada hora por país/ASN**

Para ver las descripciones de los registros, vaya a Descripciones e informes de registros de radar para proveedores de servicios y empresas

Habilitar informes de plataforma

Haga clic en el botón de alternancia para habilitar o inhabilitar los informes que quiere recibir. Si inhabilitas un informe existente, no se generan registros nuevos, pero los informes antiguos permanecen en la ubicación actual.



Mejor Informe Anónimo para Plataformas

- Estos informes ayudan a los proveedores a comparar su rendimiento con el de otras plataformas dentro de su grupo de pares, es decir, dentro del mismo país, región o ASN.
- Los datos de rendimiento de los 15 principales proveedores del grupo de pares se agregan en función de las mismas categorías. La mejor opción aparece junto a la mejor relación calidad-precio del proveedor específico.
- Anonymous Best Report for SSL Platforms está disponible para que su rendimiento se pueda comparar con otras plataformas SSL.
- Las direcciones IP del cliente se truncan a /28.
- Los resultados del "mejor"proveedor ayudan a las nube/CDN a centrar los esfuerzos de rendimiento en ASN de gran volumen o críticas para el negocio que son competitivamente débiles para sus pares.
- El informe proporciona detalles sobre el rendimiento desglosado por IP de resolución de DNS, IP de cliente /28 y nodo de almacenamiento en caché que sirvió los objetos. Lo mismo se compara con la "mejor"plataforma para los mismos criterios.

Disponible para RTT y rendimiento.

- Para obtener las descripciones de los registros, consulte Descripciones e informes de registros de radar para proveedores de servicios y empresas.

Informe de ID de nodo de caché para plataformas

- Este informe se utiliza para identificar el servidor o centro de datos específico que respondió a una solicitud y ayudar a diagnosticar problemas del servidor.
- Proporciona el ID del centro de datos o del equipo que respondió a una solicitud específica.
- Ayuda a entender por qué el rendimiento a través de un nodo específico (POP o máquina, o ID de nodo), era bueno o malo.

- El rendimiento consiste en el tiempo de respuesta, el rendimiento, la disponibilidad (tipo de sonda), la IP de resolución de DNS, la IP de cliente /28 y el nodo de almacenamiento en caché que sirvió los objetos.
- Para ver las descripciones de los registros, consulte [Radar Log Descriptions and Reports for Service Providers and Enterprises] (#radar-log-descriptions-and-reports-for-service-providers-and-enterprises)

Cada hora por país/ASN

- Este informe ayuda a verificar si el rendimiento de sus proveedores varía significativamente durante un día.
- Muestra la hora en que se tomaron las mediciones truncadas hasta la hora; por ejemplo. `2018-03-11T23:00:00`.
- Para obtener las descripciones de los registros, consulte Descripciones e informes de registros de radar para proveedores de servicios y empresas.

Informes de red

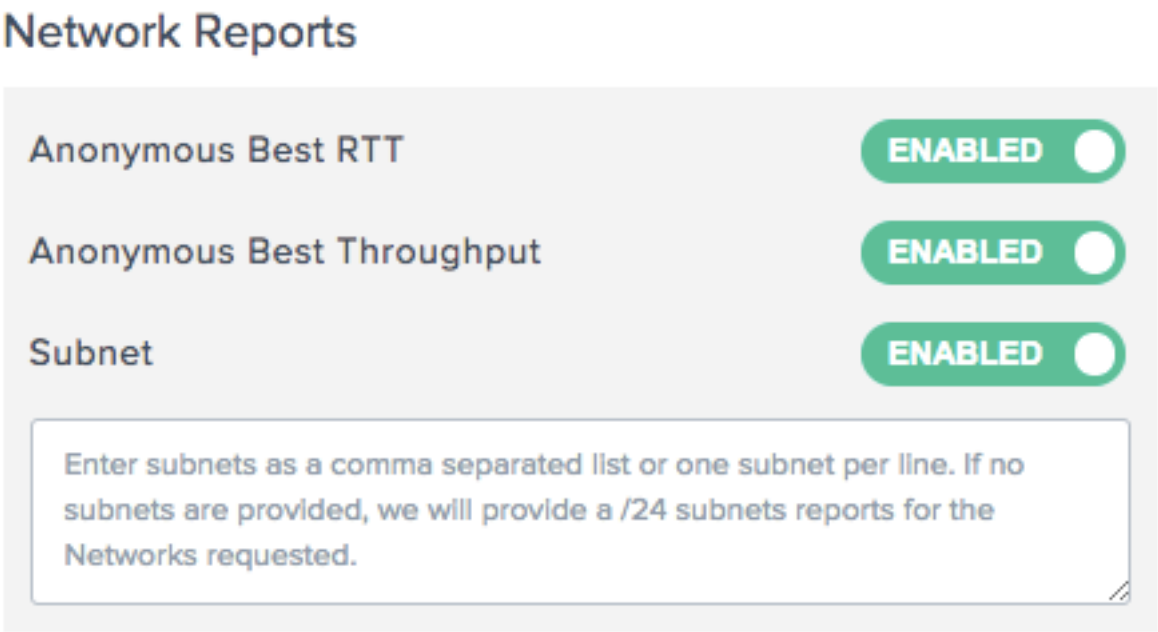
Existen tres tipos de **informes de red**:

1. **Mejor anónimo para el tiempo de ida y vuelta (RTT)**
2. **Mejor anónimo para el rendimiento**
3. **Subred**

Para obtener las descripciones de los registros, consulte Descripciones e informes de registros de radar para ISP.

Habilitar informes de red

Haga clic en el botón de alternancia para habilitar o inhabilitar los informes que quiere recibir. Cuando está inhabilitada, los registros nuevos dejan de generarse, pero hay informes antiguos.
Para generar un informe de subred, introduzca las subredes específicas de las redes. Si no se ha introducido ninguna subred, los informes se generan con el bloque de CIDR de ASN como subred predeterminada.



Mejor informe anónimo para ISP

- En el informe Anonymous Best for ISP, se utiliza un grupo de pares para la comparación "mejor" . El grupo de pares se basa en la ubicación del ISP. Por lo general, son los 10 ISP más medidos en un país específico, con un mínimo de más de 1000 sesiones.
- Los resultados del "mejor"ISP ayudan a los ISP a centrar sus esfuerzos de rendimiento en plataformas de gran volumen o críticas para el negocio y en áreas que son competitivamente débiles para sus pares.
- El informe proporciona detalles sobre el desempeño desglosado por geografía y plataforma, y lo compara con el "mejor"proveedor de servicios de Internet para los mismos criterios.
- Disponible para RTT y rendimiento.
- Para obtener las descripciones de los registros, consulte Descripciones e informes de registros de radar para ISP.

Informe de subred para ISP

- Este informe proporciona a los ISP información sobre el rendimiento de las subredes específicas de sus redes para los usuarios a través de las plataformas que medimos.
- Proporciona información sobre el proveedor de servicios que respondió a una solicitud específica.
- Ayuda a comprender el rendimiento de una subred de red.

- El rendimiento consiste en el tiempo de respuesta, el rendimiento, la disponibilidad (tipos de sondeos), la IP de resolución de DNS, la IP de cliente /28 y la subred del usuario.
- Para obtener las descripciones de los registros, consulte Descripciones e informes de registros de radar para ISP.

Registros de Radar

- Los registros de Radar están disponibles para Plataformas y Redes.
- Incluyen un subconjunto de los campos disponibles en los registros sin procesar, con algunos datos anonimizados: IP cliente /28, Referer MD5 hash.
- Se proporcionan todas las medidas tomadas para plataformas públicas, independientemente de la página que generó la medición.

> **NOTA:**
>
> NEM nunca expone las IP de cliente completas. En su lugar, expone el /28. Por ejemplo, una IP de 255.255.255.255 se muestra en un informe como 255.255.255.240/28.

Frecuencia de registro

Los registros de Radar se pueden generar diariamente (cada 24 horas) es decir, final del día, hora UTC. Los registros también se pueden generar en tiempo real (minuto a minuto).

Formato de archivo

Elija **TSV o JSON** para recibir registros e informes en cualquiera de estos formatos.

Tipo de medición

Puede configurar registros para los siguientes tipos de medida: Disponibilidad, Tiempo de Respuesta y Rendimiento. En el informe, 1: Disponibilidad, 0: Tiempo de respuesta HTTP y 14: Rendimiento HTTP.

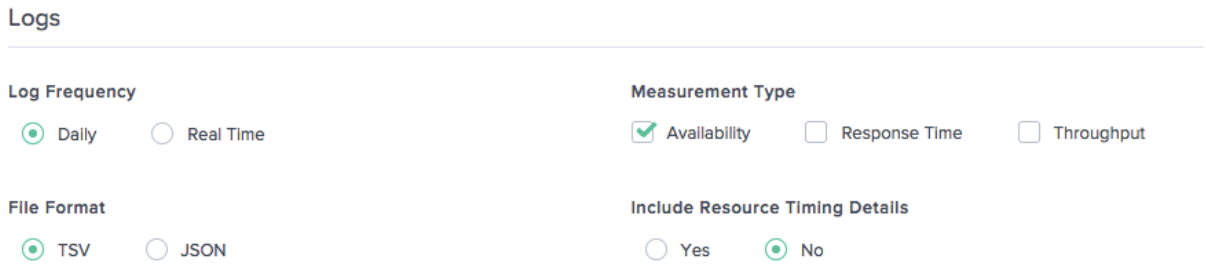
Detalles de temporización de recursos

Puede optar por incluir también detalles de temporización de recursos haciendo clic en los botones **Sí** o No. Los detalles de temporización de recursos incluyen:

- Hora de búsqueda de DNS
- Hora de conexión TCP

- Tiempo de conexión seguro
- Tiempo de descarga

Para obtener las descripciones de los registros, consulte Descripciones e informes de registros de radar para proveedores de servicios y empresas.



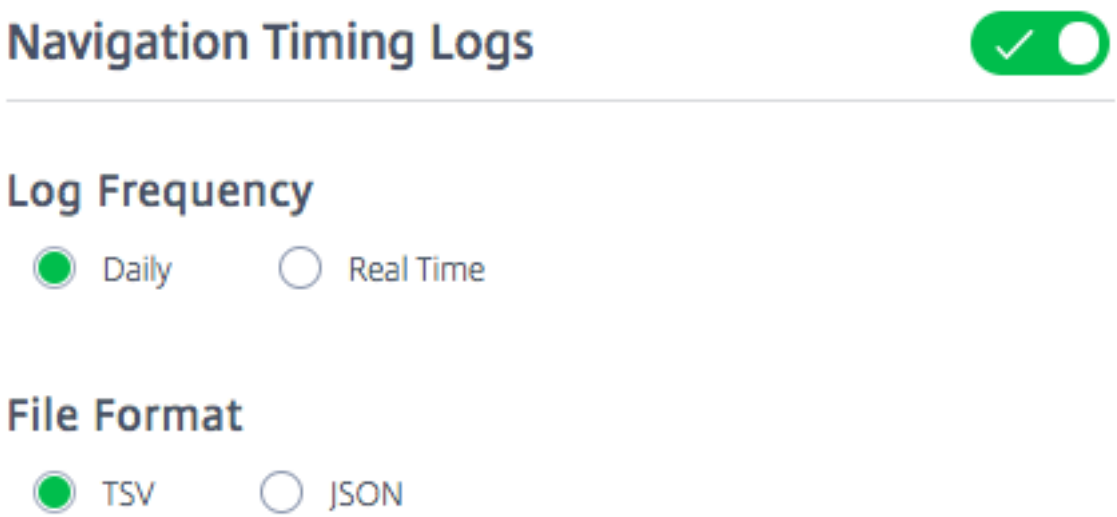
Registros de sincronización de navegación

Frecuencia de registro

Los registros de sincronización de navegación se pueden generar diariamente (cada 24 horas) es decir, final del día, hora UTC. Los registros también se pueden generar en tiempo real (minuto a minuto).

Formato de archivo

Elija **TSV** o **JSON** para recibir registros de sincronización de navegación en cualquiera de estos formatos. Para obtener las descripciones de los registros, consulte Descripciones del registro de sincronización



Registros de Openmix

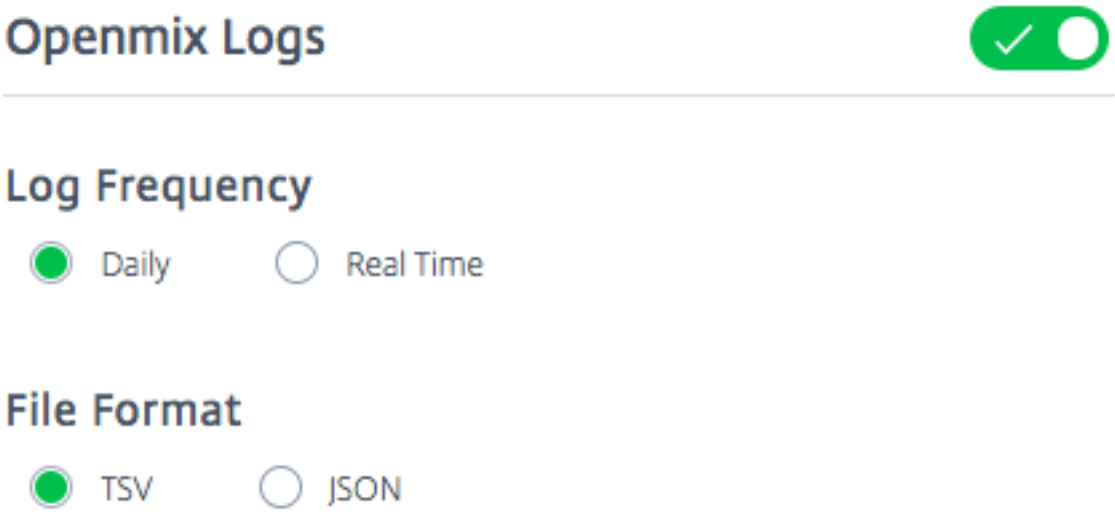
Frecuencia de registro

Los registros de Openmix se generan en tiempo real (es decir, minuto a minuto). Estos registros proporcionan mediciones en tiempo real tomadas para los clientes de Openmix.

Formato de archivo

Elija **TSV** o **JSON** para recibir registros Openmix y HTTP Openmix en cualquiera de estos formatos. JSON es sin embargo el formato recomendado.

Para ver las descripciones de los registros, consulte Descripciones de los registrosde



Entrega de servicios en la nube

Esta opción le permite seleccionar el modo de entrega. Puede optar por recibir registros e informes en el depósito de AWS S3 o en el depósito de Google Cloud Storage (GCS).
Puede acceder a los depósitos de S3 y GCS con la información de inicio de sesión proporcionada y usar s3cmd o la CLI de AWS para S3 y la línea de comandos de gsutil para GCS.

AWS S3

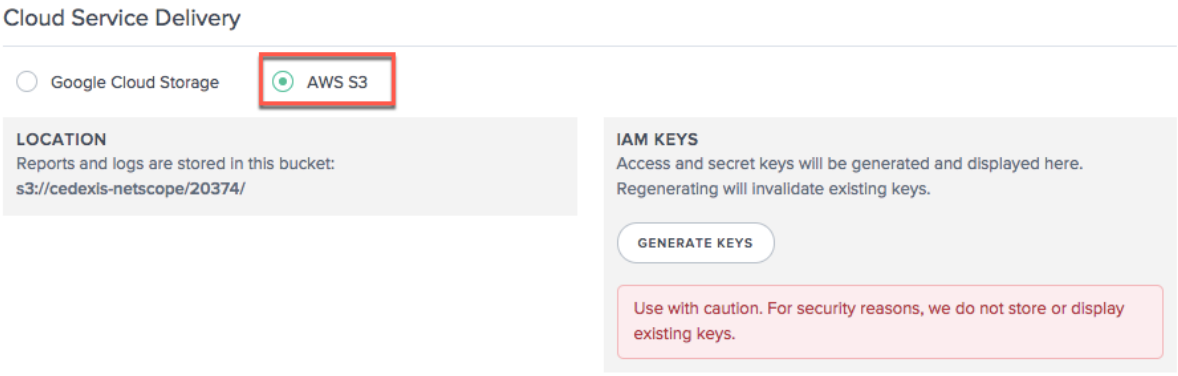
Para los registros e informes que se entregarán al depósito de AWS S3, seleccione **AWS S3**.

Ubicación La ubicación representa el depósito en AWS S3 donde se guardan los registros y los informes.

Claves de IAM Si selecciona el botón **Generar claves** en AWS S3, las claves de IAM de AWS (claves de acceso y secretas) se generan y se muestran en Claves de IAM. Asegúrese de grabar las claves porque no están guardadas en ningún lugar para verlas más tarde.

> **NOTA:**
>
> El par de claves de acceso y secreto son la única copia de las claves privadas. El cliente debe almacenarlos de forma segura. La regeneración de las nuevas claves invalida las existentes.
> El archivo de configuración S3cmd reconoce las claves de acceso (recibidas a través de la interfaz de usuario del portal) y ayuda al cliente a conectarse al depósito S3. La CLI de AWS debe instalarse en la máquina del cliente para conectarse a S3.

Para obtener información sobre cómo usar las claves de acceso y secretas con s3cmd para descargar informes del bucket de S3, consulte las preguntas frecuentes.



Almacenamiento en la nube de Google

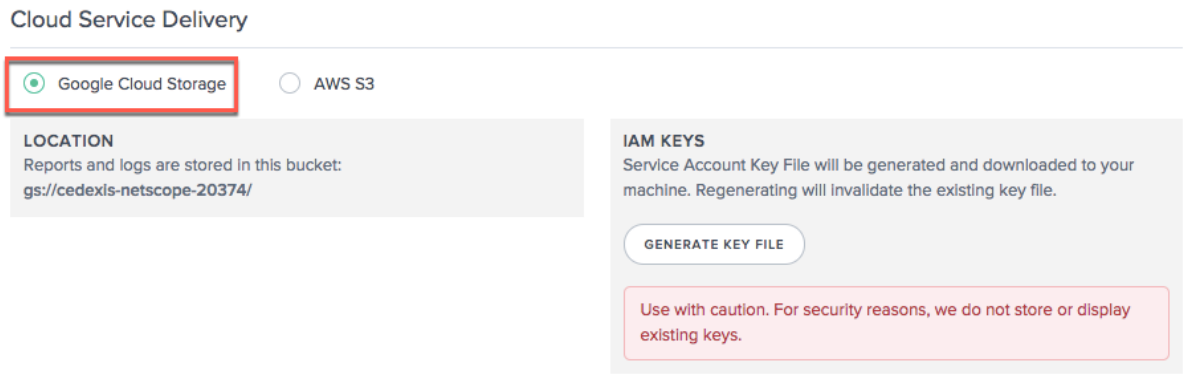
Para que los registros e informes se entreguen a GCS, selecciona **Google Cloud Storage**.

Ubicación La ubicación representa el depósito en Google Cloud Storage donde se guardan los registros y los informes.

Claves de IAM Al seleccionar el botón **Generar archivo de clave**, el archivo de clave de cuenta de Google Service se descarga en el equipo.

> **NOTA:**
>
> Este archivo de clave sirve como única copia de la clave privada. Tome nota de la dirección de correo electrónico de su cuenta de servicio y almacene de forma segura el archivo de clave privada de la cuenta de servicio. La regeneración de un nuevo archivo de clave invalida el archivo existente.

Este archivo clave se puede utilizar con la herramienta gsutil para descargar registros e informes desde el depósito GCS. Para obtener más información sobre cómo usar el archivo de claves para descargar archivos de registro, consulte las preguntas frecuentes.



Descripciones e informes del registro de Radar para proveedores de servicios y empresas

Registros de Radar para proveedores

- Estos registros proporcionan mediciones de Radar para socios de referencia.
- Proporcionan todas las medidas tomadas para plataformas públicas, independientemente de la página que generó la medición.
- Los registros de Radar incluyen un subconjunto de los campos disponibles en los registros sin procesar, con algunos datos anonimizados: IP cliente /28, Referer MD5 hash.
- Este es un ejemplo de uso compartido de registro de radar de plataforma en formato de archivo TSV.

> **NOTA:**
>
> - NEM nunca expone las IP de cliente completas. En su lugar, expone el /28. Por ejemplo, una IP de 255.255.255.255 se muestra en un informe como 255.255.255.240/28.
> - La información GEO del cliente se extrae en función de la IPv4 del cliente, que es más detallada.

Descripciones de registro Los siguientes son los encabezados de las columnas y las descripciones de los registros de radar. Los campos aparecen en el siguiente orden en los archivos de salida:

Registro	Descripción
Timestamp	Es la hora UTC de la solicitud en formato AAAA-MM-DDTHH:MI:SSZ. El valor real (hasta el segundo) en las tablas de registro se redondea a la hora más cercana (30-03-2018 T 23:00:00 Z) o al día (30-03-2018 T 00:00:00 Z) en las tablas de horas/días, respectivamente. La marca de tiempo siempre está en UTC en todos los conjuntos de datos.
ID de nodo único	También se conoce como ID de nodo de caché. Es un valor arbitrario. Por lo general, una IP que los servidores perimetrales de CDN devuelven para ayudar a las CDN a identificar internamente qué servidor gestionó una solicitud en particular". (cadena vacía): Proviene de clientes de Radar que no admiten la detección de UNI. 0: El agente de usuario no admite las funciones necesarias para la detección de UNI. 1: El cliente encontró un error durante la detección de UNI, como HTTP 404 u otra respuesta fallida. 2: Se intentó la detección de UNI, pero se produjo un error.
ID de proveedor	ID interno de la plataforma que se está midiendo.
Tipo de sonda	El tipo de sondeo que se está midiendo (por ejemplo, 1: Tiempo de conexión HTTP, 0: Tiempo de respuesta HTTP, 14: Rendimiento HTTP, etc.). Para indicar que el servicio está disponible, utilice la información devuelta correctamente dentro del tiempo permitido.

Registro	Descripción
Código de respuesta	Resultado de la medición. Por ejemplo, 0: éxito, 1: tiempo de espera agotado, 4: error. Para los cálculos de disponibilidad, el porcentaje de mediciones se toma con una respuesta de 0 (éxito) frente al número total de mediciones (total, independientemente de la respuesta). Para otros tipos de sonda (RTT y rendimiento), el filtro solo debe tener en cuenta los puntos de datos RTT con un código de éxito 0 al calcular las estadísticas en el RTT. Lo mismo para el rendimiento.
Valor de medición	El valor de medición registrado, cuyo significado varía según el tipo de sonda. Representa mediciones de disponibilidad (1)/Tiempo de respuesta (0) en milisegundos y Rendimiento (14) en kbps.
Mercado de Resolver	El mercado del solucionador DNS que manejó la solicitud. Generalmente el continente donde se encuentra el solucionador DNS, donde, 0: Desconocido (XX), 1:América del Norte (NA) 5: África (AF), 3: Europa (UE), 4: Asia (AS), 2: Oceanía (OC), 6: América del Sur (SA).
País de resolución	El país del solucionador DNS que manejó los request.ID se puede asignar a nombres enhttps://community-radar.citrix.com/ref/countries.json.gz
Región de resolución	La región del solucionador de DNS que gestionó los IDs de solicitud se puede asignar a los nombres en https://community-radar.citrix.com/ref/regions.json.gz **Nota:** No todos los países del mundo tienen regiones definidas.
Estado de resolución	El estado de la resolución de DNS que gestionó los IDs de solicitud se puede asignar a los nombres en https://community-radar.citrix.com/ref/states.json.gz Nota: No todos los países del mundo tienen estados definidos.

Registro	Descripción
Ciudad de Resolver	La ciudad de la resolución de DNS que gestionó la solicitud. La ciudad de resolución se agrega buscando una dirección IP de resolución. Los ID se pueden asignar a los nombres en https://community-radar.citrix.com/ref/cities.json.gz
ASN de resolución	Número de sistema autónomo (ASN) del solucionador DNS que gestionó la solicitud. Por lo general, la ASN que tiene los ID de resolución de DNS se puede asignar a los nombres de https://community-radar.citrix.com/ref/asns.json.gz
Resolución IP	La dirección IP del solucionador DNS desde el que nuestra infraestructura recibió la solicitud DNS.
Mercado de clientes	El mercado del usuario final que generó esta medición. Generalmente el continente donde se encuentra la IP del cliente; donde, 0: Desconocido (XX), 1:América del Norte (NA) 5: África (AF), 3: Europa (UE), 4: Asia (AS), 2: Oceanía (OC), 6: América del Sur (SA).
País del cliente	El país del usuario final que generó esta medida. IDs se puede asignar a nombres enhttps://community-radar.citrix.com/ref/countries.json.gz
Región del cliente	La región del usuario final que generó esta medida. Por lo general, la región geográfica en la que se encuentra la IP del cliente. Los ID se pueden asignar a los nombres en https://community-radar.citrix.com/ref/regions.json.gz Nota: No todos los países del mundo tienen regiones definidas.
Estado del cliente	El estado del usuario final que generó esta medida. Por lo general, el estado donde se encuentra la IP del cliente. Los ID se pueden asignar a los nombres en https://community-radar.citrix.com/ref/states.json.gz Nota: No todos los países del mundo tienen estados definidos.

Registro	Descripción
Ciudad del cliente	La ciudad del usuario final que generó esta medida. Generalmente, la ciudad en la que se encuentra la IP del cliente.IDs se pueden asignar a nombres enhttps://community-radar.citrix.com/ref/cities.json.gz
ASN del cliente	Número de sistema autónomo (ASN) del usuario final que generó esta medida. Por lo general, el ASN que contiene los IP.IDs del cliente se puede asignar a nombres enhttps://community-radar.citrix.com/ref/asns.json.gz
Client IP	La IP del usuario final que generó esta medida.
Host de referencia MD5	La información del Referer (Protocolo, Host y Ruta) proviene del encabezado del Referer de la solicitud HTTP a Radar. El host de referencia es MD5 hash.
Agente de usuario	Es la cadena del agente de usuario de la página del explorador que aloja la etiqueta. Por ejemplo, si usa Chrome y navegas por una página con la etiqueta Radar, las mediciones de radar en segundo plano registran el agente de usuario de su explorador Chrome. Las medidas incluyen el explorador Chrome, la versión de Chrome, información sobre el sistema operativo en el que se ejecuta Chrome, etc.
Tiempo de búsqueda DNS (opcional)	Con la API Resource Timing, se calcula la diferencia entre el final de la búsqueda de dominio y el inicio de la búsqueda de dominio. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como domainLookupEnd - domainLookupStart.
Hora de conexión TCP (opcional)	Con la API Resource Timing, se calcula la diferencia entre Connect End y Connect Start. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como connectEnd - connectStart.

Registro	Descripción
Tiempo de conexión segura (opcional)	Con la API Resource Timing, se calcula la diferencia entre Connect End y Secure Connection Start. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como connectEnd - secureConnectionStart.
Latencia (opcional)	Con la API Resource Timing, se calcula la diferencia entre el inicio de la respuesta y el inicio de la solicitud. Calcula cuándo ambos valores no son nulos y la hora de inicio de la respuesta es mayor que la hora de inicio de la solicitud. Se calcula como responseStart - requestStart
Tiempo de descarga (opcional)	Con la API Resource Timing, se calcula la diferencia entre el final de la respuesta y el inicio de la respuesta. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como responseEnd - responseStart.
Perfil del cliente	Este campo ayuda a identificar si los datos provienen de aplicaciones móviles o exploradores. También nos permite diferenciar entre iOS, aplicaciones Android y exploradores. Se utiliza un número para identificar cada perfil de cliente. Los valores de este campo son: null, 0, 1, 2, 3, 4. Donde, null: Generalmente implica un cliente Radar anterior que no admite el envío del valor client_profile. 0: Explorador; 1: iOS - Radar Runner para la aplicación iOS escrita en Swift; 2: Android; 3: Explorador en la versión móvil del sitio web; 4: iOS - Radar Runner para la aplicación iOS escrita en Objective-C.
Versión del perfil del cliente	La versión del perfil del cliente nos dice qué versión del código Radar Runner (para iOS) o AndroidRadar SDK (para Android) se utilizó en la aplicación móvil. Este campo está destinado únicamente para uso interno.

Registro	Descripción
Categoría de dispositivo	Todos los dispositivos se clasifican en uno de los siguientes: Smartphone, Tablet, PC, Smart TV y Otros. 'Otro'se utiliza como valor predeterminado si el analizador no puede determinar el valor de cualquiera de los campos.
Dispositivo	El tipo de dispositivo en el que se encuentra el usuario, por ejemplo, un iPhone de Apple. La cadena del agente de usuario lo detecta desde el explorador que se ejecuta en la página que aloja la etiqueta Radar.
Explorador web	El tipo de explorador que está utilizando el usuario, por ejemplo Mobile Safari UI/WKWebView 0.0.0. La cadena del agente de usuario lo detecta desde el explorador que se ejecuta en la página que aloja la etiqueta Radar.
SO	El sistema operativo utilizado. Por ejemplo, iOS 11.0.3. La cadena de agente de usuario lo detecta desde el explorador que se ejecuta en la página que aloja la etiqueta Radar.
IP del cliente de informes	Esta IP es la IP pública enmascarada /48 del usuario que realiza la medición. Puede ser IPv4 o IPv6 (si es compatible).

Mejor informe anónimo

- Los mejores informes anónimos ayudan a los proveedores a comparar su rendimiento con el grupo de pares de la otra plataforma, es decir, dentro del mismo país, región o ASN.
- Los datos de rendimiento de los 15 principales proveedores del grupo de pares se agregan en función de las mismas categorías. La mejor opción aparece junto a la mejor relación calidad-precio del proveedor específico.
- Anonymous Best Report for SSL Platforms está disponible para que su rendimiento se pueda comparar con otras plataformas SSL.
- Las direcciones IP del cliente se truncan a /28.
- Los resultados del "mejor"proveedor ayudan a las nube/CDN a centrar los esfuerzos de rendimiento en ASN de gran volumen o críticas para el negocio que son competitivamente débiles para sus pares.
- El informe proporciona detalles sobre el rendimiento, que consiste en IP de resolución de DNS,

IP de cliente /28 y el nodo de almacenamiento en caché que sirvió los objetos. Se compara con la “mejor”plataforma para los mismos criterios.

- Disponible para RTT o Rendimiento.
- El siguiente es un ejemplo de mejor informe anónimo de plataforma para RTT en formato de archivo TSV.

Descripciones de registro A continuación se muestran los encabezados de las columnas y las descripciones del mejor informe anónimo. Los campos aparecen en el siguiente orden en los archivos de salida.

Registro	Descripción
País de resolución	País del solucionador DNS que gestionó la solicitud.
Región de resolución	La región del solucionador DNS que gestionó la solicitud.
Estado de resolución	El estado del solucionador DNS que manejó la solicitud.
ID de ASN del solucionador	Número de sistema autónomo del solucionador DNS que gestionó la solicitud. Por lo general, la ASN que tiene el solucionador de DNS.
Nombre ASN del solucionador	El nombre de la ASN.
Resolución IP	La dirección IP del solucionador DNS desde el que nuestra infraestructura recibió la solicitud DNS.
País del cliente	País del usuario final que generó esta medida.
Región del cliente	La región del usuario final que generó esta medida.
Estado del cliente	El estado del usuario final que generó esta medida.
ID de ASN del cliente	Número de sistema autónomo (ASN) del usuario final que generó esta medida. Por lo general, la ASN que tiene la IP del cliente.
Nombre de ASN del cliente	El nombre de la ASN del usuario final que generó la medida.
Client IP	La IP del usuario final que generó la medición.
Éxitos	Número total de mediciones que tuvieron éxito.Consejo: Éxito/Total == Disponibilidad.

Registro	Descripción
Tiempos de espera	El número de mediciones que se agotó el tiempo de espera.
Errores	El número de mediciones que fueron errores.
Total	El número total de medidas.
Media	El promedio de todos los valores de medición de esa fila.
Mejor Media	El mejor medio entre los 15 principales proveedores del grupo de pares.
Mediciones de la mejor media	Número total de mediciones que produjeron el mejor recuento de medias.
Mediana	El valor del percentil 50 es el valor medio de las mediciones para un proveedor en particular, cuando las mediciones se enumeran en orden.
Mejor mediana	El mejor valor del percentil 50 (por debajo del cual se encuentra el 50 por ciento de las mediciones) de los 15 principales proveedores del grupo de pares.
Mediciones de la mejor media	Número total de medidas que produjeron la mejor mediana
5th	El valor del 5.º percentil para el proveedor.
Mejor 5.º	El mejor valor del 5.º percentil de los 15 principales proveedores del grupo de pares.
Las mejores 5.ª medidas	Número total de medidas que produjeron el best_5th
10th	Valor del percentil 10 para el proveedor.
Mejor 10.º	El mejor valor del 10.º percentil de los 15 principales proveedores del grupo de pares.
Mejores 10.ª medidas	Número total de medidas que produjeron el best_10th
90th	Valor del percentil 90 para el proveedor.
Mejor 90.ª	El mejor valor del percentil 90 de los 15 principales proveedores del grupo de pares.
Las mejores medidas 90	Número total de medidas que produjeron el best_90th
95th	Valor del percentil 95 para el proveedor.

Registro	Descripción
Mejor 95.ª	El mejor valor del percentil 95 de los 15 principales proveedores del grupo de pares.
Las mejores 95.ª medidas	Número total de medidas que produjeron el best_95th
Stdev	La desviación estándar para el proveedor
Mejor Stdev	La mejor desviación estándar de los 15 principales proveedores del grupo de pares.
Las mejores medidas de Stdev	Número total de mediciones que produjeron el mejor std.dev.
Disponibilidad	La disponibilidad en porcentaje para el proveedor. La disponibilidad es la tasa de éxito del sondeo, es decir, éxitos/(Éxitos + Falla + Tiempos de espera)
Mejor disponibilidad	El mejor valor de disponibilidad entre los 15 principales proveedores del grupo de pares.
Mejores mediciones de disponibilidad	El número de mediciones que produjeron la mejor disponibilidad
Importancia	Valores sintéticos generados para ayudar a encontrar datos accionables.
ID de nodo único	Estos ID son una lista separada por comas de los ID de nodo únicos para las mediciones de esa fila.
Tipo de medición	El valor de medición registrado, cuyo significado varía según el tipo de sonda. Es HTTP_COLD (disponibilidad), HTTP_RTT (tiempo de ida y vuelta) o HTTP_KBPS (rendimiento).
ID de proveedor	El número de ID ITM interno de NetScaler de ese proveedor.

Informe de ID de nodo de caché (anteriormente Informe de proveedor de servicios múltiples)

Este informe se utiliza para identificar el servidor o centro de datos específico que respondió a una solicitud y ayudar a diagnosticar problemas del servidor.

- Proporciona el ID del centro de datos o del equipo que respondió a una solicitud específica.
- Ayuda a entender por qué el rendimiento a través de un nodo específico (POP o máquina, o ID de nodo), era bueno o malo.

- El rendimiento consiste en el tiempo de respuesta, el rendimiento, la disponibilidad (tipo de sonda), la IP de resolución de DNS, la IP de cliente /28 y el nodo de almacenamiento en caché que sirvió los objetos.
- El siguiente es un ejemplo de informe de ID de nodo de caché de plataforma en formato de archivo TSV.

Descripciones de registro A continuación se muestran los encabezados de las columnas y las descripciones del informe de ID de nodo de caché. Los campos aparecen en el siguiente orden en los archivos de salida:

Registro	Descripción
Nombre del proveedor	Es el nombre del proveedor que se está midiendo.
Valor de medición	El valor de medición registrado, cuyo significado varía según el tipo de sonda. Se trata de mediciones connect (1) /RTT (0) en milisegundos y mediciones de rendimiento (14) en kbps.
ID de nodo único	Se conoce como ID de nodo de caché. Un valor arbitrario, normalmente una IP que los servidores perimetrales de CDN devuelven para ayudar a las CDN a identificar internamente qué servidor gestionó una solicitud en particular". (cadena vacía): Proviene de clientes de Radar que no admiten la detección de UNI. 0: El agente de usuario no admite las funciones necesarias para la detección de UNI. 1: El cliente encuentra un error durante la detección de UNI, como HTTP 404 u otra respuesta fallida. 2: Se intentó la detección de UNI, pero produjo un error.
País de resolución	País del solucionador DNS que gestionó la solicitud.
Región de resolución	La región del solucionador DNS que gestionó la solicitud.
Estado de resolución	El estado del solucionador DNS que manejó la solicitud.
ASN de resolución	Número de sistema autónomo del solucionador DNS que gestionó la solicitud. Por lo general, la ASN que tiene el solucionador de DNS.
Nombre ASN del solucionador	El nombre de la ASN.

Registro	Descripción
Resolución IP	La dirección IP del solucionador DNS desde el que nuestra infraestructura recibió la solicitud DNS.
País del cliente	País del usuario final que generó esta medida.
Región del cliente	La región del usuario final que generó esta medida.
Estado del cliente	El estado del usuario final que generó esta medida.
ASN del cliente	Número de sistema autónomo (ASN) del usuario final que generó esta medida. Por lo general, la ASN que tiene la IP del cliente.
Nombre de ASN del cliente	El nombre de la ASN del usuario final que generó la medida.
Client IP	La IP del usuario final que generó la medición.
Operación correctamente realizada.	Número total de mediciones que tuvieron éxito.Consejo: Éxito/Total == Disponibilidad.
Tiempo de espera	El número de mediciones que se agotó el tiempo de espera.
Error	El número de mediciones que fueron errores.
Total	El número total de medidas.
Media	El promedio de los valores de medición para cada fila.
Mediana	El valor del percentil 50 es el valor medio de las mediciones para un proveedor en particular, cuando las mediciones se enumeran en orden.
5th	El valor del 5.º percentil para el proveedor.
10th	Valor del percentil 10 para el proveedor.
90th	Valor del percentil 90 para el proveedor.
95th	Valor del percentil 95 para el proveedor.
Stdev	La desviación estándar para el proveedor.
Disponibilidad	La disponibilidad en porcentaje para el proveedor.
Importancia	Valores sintéticos generados para ayudar a encontrar datos accionables.

Informe cada hora por país/ASN

- Este informe ayuda a verificar si el rendimiento de sus proveedores varía significativamente durante un día.
- Muestra la hora en que se tomaron las mediciones truncadas hasta la hora; por ejemplo. `2018-03-11T23:00:00`.
- El siguiente es un ejemplo de informe de plataforma por hora por país/ASN en formato de archivo TSV.

Descripciones de registro A continuación se muestran los encabezados de las columnas y las descripciones del informe Cada hora por país/ASN. Los campos aparecen en el siguiente orden en los archivos de salida:

Registro	Descripción
Marca de tiempo 60 minutos	La hora UTC en la que se tomaron las mediciones truncada hasta la hora, por ejemplo2018-03-11T 23:00:00.
Nombre del proveedor	Es el nombre del proveedor que se está midiendo.
Tipo de medición	El valor de medición registrado, cuyo significado varía según el tipo de sonda. Es HTTP_COLD (disponibilidad), HTTP_RTT (tiempo de ida y vuelta) o HTTP_KBPS (rendimiento).
País del cliente	País del usuario final que generó esta medida.
ASN del cliente	Número de sistema autónomo (ASN) del usuario final que generó esta medida. Por lo general, la ASN que tiene la IP del cliente.
Nombre de ASN del cliente	El nombre de la ASN del usuario final que generó la medida.
Operación correctamente realizada.	Número total de mediciones que tuvieron éxito.Consejo: Éxito/Total == Disponibilidad.
Tiempo de espera	El número de mediciones que se agotó el tiempo de espera.
Error	El número de mediciones que fueron errores.
Total	El número total de medidas.
Media	El promedio de los valores de medición para cada fila.

Registro	Descripción
Mediana	El valor del percentil 50 es el valor medio de las mediciones para un proveedor en particular, cuando las mediciones se enumeran en orden.
5th	El valor del 5.º percentil para el proveedor.
10th	Valor del percentil 10 para el proveedor.
90th	Valor del percentil 90 para el proveedor.
95th	Valor del percentil 95 para el proveedor.
Stdev	La desviación estándar para el proveedor.
Disponibilidad	La disponibilidad en porcentaje para el proveedor.
Importancia	Valor sintético generado para ayudar a encontrar datos accionables.
ID de proveedor	El número de ID ITM interno de NetScaler de ese proveedor.

Descripciones e informes de registro de Radar para ISP

Registros de Radar para ISP

Los registros de radar permiten a los ISP medir su rendimiento con respecto a las plataformas globales en detalle. Los ISP pueden usar estos datos para encontrar áreas en las que se deben realizar mejoras o para verificar el rendimiento esperado.

- Proporciona acceso a las mediciones de Radar.
- Proporciona mediciones tomadas de ISP en plataformas públicas, independientemente de la página que generó la medición.
- Los registros de Radar incluyen un subconjunto de los campos disponibles en los registros sin procesar, con algunos datos anonimizados: IP cliente /28, referer MD5 hash.
- Los archivos de registro están en formato TSV.
- El siguiente es un ejemplo de Network Radar Log Share en formato de archivo TSV.

Descripciones de registro Los siguientes son los encabezados de las columnas y las descripciones de los registros de Radar para ISP. Los campos aparecen en el siguiente orden en los archivos de salida.

Registro	Descripción
Timestamp	Es la hora UTC de la solicitud en formato AAAA-MM-DDTHH:MI:SSZ. El valor real (hasta el segundo) en las tablas de registro se redondea a la hora más cercana (30-03-2018 T 23:00:00 Z) o al día (30-03-2018 T 00:00:00 Z) en las tablas de horas/días, respectivamente. La marca de tiempo siempre está en UTC en todos los conjuntos de datos.
ID de proveedor	ID interno de la plataforma que se está midiendo.
Tipo de sonda	El tipo de sondeo que se está midiendo (por ejemplo, 1: Tiempo de conexión HTTP, 0: Tiempo de respuesta HTTP, 14: Rendimiento HTTP, etc.). La información que devolvió correctamente dentro del tiempo permitido se utiliza para indicar que el servicio está disponible.
Código de respuesta	Resultado de la medición. Por ejemplo, 0: éxito, 1: tiempo de espera agotado, 4: error. Para los cálculos de disponibilidad, el porcentaje de mediciones se toma con una respuesta de 0 (éxito) frente al número total de mediciones (total). Para otros tipos de sonda (RTT y rendimiento), el filtro solo debe tener en cuenta los puntos de datos RTT con un código de éxito 0 al calcular las estadísticas en el RTT. Lo mismo para el rendimiento.
Valor de medición	El valor de medición registrado, cuyo significado varía según el tipo de sonda. Se trata de mediciones de disponibilidad (1) /tiempo de respuesta (0) en milisegundos y rendimiento (14) en kbps.
Mercado de Resolver	El mercado del solucionador DNS que manejó la solicitud. Generalmente el continente donde se encuentra el solucionador DNS, donde, 0: Desconocido (XX), 1:América del Norte (NA) 5: África (AF), 3: Europa (UE), 4: Asia (AS), 2: Oceanía (OC), 6: América del Sur (SA).

Registro	Descripción
País de resolución	El país de la resolución de DNS que gestionó los ID de solicitud se puede asignar a los nombres de https://community-radar.citrix.com/ref/countries.json.gz
Región de resolución	La región del solucionador de DNS que gestionó los ID de solicitud se puede asignar a los nombres de https://community-radar.citrix.com/ref/regions.json.gz. No todos los países del mundo tienen regiones definidas.
Estado de resolución	El estado del solucionador de DNS que gestionó los ID de solicitud se puede asignar a los nombres de https://community-radar.citrix.com/ref/states.json.gz. No todos los países del mundo tienen estados definidos.
ASN de resolución	Número de sistema autónomo (ASN) del solucionador DNS que gestionó la solicitud. Por lo general, la ASN que tiene los ID de resolución de DNS se puede asignar a los nombres de https://community-radar.citrix.com/ref/asns.json.gz.
Resolución IP	La dirección IP del solucionador DNS desde el que nuestra infraestructura recibió la solicitud DNS.
Mercado de clientes	El mercado del usuario final que generó esta medición. Generalmente el continente donde se encuentra la IP del cliente; donde, 0: Desconocido (XX), 1:América del Norte (NA) 5: África (AF), 3: Europa (UE), 4: Asia (AS), 2: Oceanía (OC), 6: América del Sur (SA).
País del cliente	El país del usuario final que generó esta medida. IDs se puede asignar a nombres enhttps://community-radar.citrix.com/ref/countries.json.gz

Registro	Descripción
Región del cliente	La región del usuario final que generó esta medida. Por lo general, la región geográfica en la que se encuentra la IP del cliente. Los ID se pueden asignar a los nombres de https://community-radar.citrix.com/ref/regions.json.gz. No todos los países del mundo tienen regiones definidas.
Estado del cliente	El estado del usuario final que generó esta medida. Generalmente, el estado en el que se encuentra la IP del cliente. Los ID se pueden asignar a los nombres de https://community-radar.citrix.com/ref/states.json.gz. No todos los países del mundo tienen estados definidos.
ASN del cliente	Número de sistema autónomo (ASN) del usuario final que generó esta medida. Por lo general, la ASN que tiene la IP del cliente. Los ID se pueden asignar a nombres en https://community-radar.citrix.com/ref/asns.json.gz
Client IP	La IP del usuario final que generó esta medida.
Host de referencia MD5	La información del Referer (Protocolo, Host y Ruta) proviene del encabezado del Referer de la solicitud HTTP a Radar. El host de referencia es MD5 hash.
Agente de usuario	Es la cadena del agente de usuario de la página del explorador que aloja la etiqueta. Por ejemplo, si usa Chrome y navegas por una página con la etiqueta Radar, las mediciones de radar en segundo plano registran el agente de usuario de su explorador Chrome. Las medidas incluyen el explorador Chrome, la versión de Chrome, información sobre el sistema operativo en el que se ejecuta Chrome, etc.

Registro	Descripción
Tiempo de búsqueda DNS (opcional)	Con la API Resource Timing, se calcula la diferencia entre el final de la búsqueda de dominio y el inicio de la búsqueda de dominio. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como domainLookupEnd - domainLookupStart.
Hora de conexión TCP (opcional)	Con la API Resource Timing, se calcula la diferencia entre Connect End y Connect Start. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como connectEnd - connectStart.
Tiempo de conexión segura (opcional)	Con la API Resource Timing, se calcula la diferencia entre el fin de la conexión y el inicio de la conexión segura. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como connectEnd - secureConnectionStart.
Latencia (opcional)	Con la API Resource Timing, se calcula la diferencia entre el inicio de la respuesta y el inicio de la solicitud. Calcula cuándo ambos valores no son nulos y la hora de inicio de la respuesta es mayor que la hora de inicio de la solicitud. Se calcula como responseStart - requestStart
Tiempo de descarga (opcional)	Con la API Resource Timing, se calcula la diferencia entre el final de la respuesta y el inicio de la respuesta. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como responseEnd - responseStart.

Registro	Descripción
Perfil del cliente	Este campo ayuda a identificar si los datos provienen de aplicaciones móviles o exploradores. También nos permite diferenciar entre iOS, aplicaciones Android y exploradores. Se utiliza un número para identificar cada perfil de cliente. Los valores de este campo son: null, 0, 1, 2, 3, 4. Donde, null: Generalmente implica un cliente Radar anterior que no admite el envío del valor client_profile. 0: Explorador; 1: iOS - Radar Runner para la aplicación iOS escrita en Swift; 2: Android; 3: Explorador en la versión móvil del sitio web; 4: iOS - Radar Runner para la aplicación iOS escrita en Objective-C.
Versión del perfil del cliente	La versión del perfil del cliente nos dice qué versión del código Radar Runner (para iOS) o AndroidRadar SDK (para Android) se utilizó en la aplicación móvil. Este campo está destinado únicamente para uso interno.
Categoría de dispositivo	Todos los dispositivos se clasifican en uno de los siguientes: Smartphone, Tablet, PC, Smart TV y Otros. 'Otro'se utiliza como valor predeterminado si el analizador no puede determinar el valor de cualquiera de los campos.
Dispositivo	El tipo de dispositivo en el que se encuentra el usuario, por ejemplo, un iPhone de Apple. La cadena del agente de usuario lo detecta desde el explorador que se ejecuta en la página que aloja la etiqueta Radar.
Explorador web	El tipo de explorador que está utilizando el usuario, por ejemplo Mobile Safari UI/WKWebView 0.0.0. La cadena del agente de usuario lo detecta desde el explorador que se ejecuta en la página que aloja la etiqueta Radar.
SO	El sistema operativo que se está utilizando, por ejemplo iOS 11.0.3. La cadena del agente de usuario lo detecta desde el explorador que se ejecuta en la página que aloja la etiqueta Radar.

Informe de subred para ISP

- El informe proporciona a los ISP información sobre el rendimiento de las subredes específicas de sus redes para sus usuarios a través de las plataformas medidas.
- Proporciona información sobre el proveedor de servicios que respondió a una solicitud específica.
- Ayuda a comprender el rendimiento de la subred de la red.
- El rendimiento consiste en el tiempo de respuesta, el rendimiento, la disponibilidad (tipo de sonda), la IP de resolución de DNS, la IP de cliente /28 y el nodo de almacenamiento en caché que sirvió los objetos.
- El siguiente es un ejemplo de informe de subred de red en formato de archivo TSV.

Descripciones de registro A continuación se muestran los encabezados de las columnas y las descripciones del Informe de subred para ISP. Los campos aparecen en el siguiente orden en los archivos de salida:

Registro	Descripción
Nombre de ASN	Nombre del Sistema Autónomo desde el que se tomó la medición.
Valor de medición	El valor de medición registrado, cuyo significado varía según el tipo de sonda. Se trata de mediciones connect (1) /RTT (0) en milisegundos y mediciones de rendimiento (14) en kbps.
Subred	La subred del usuario desde donde se originó la solicitud.
ASN de resolución	Número de sistema autónomo del solucionador DNS que gestionó la solicitud. Por lo general, la ASN que tiene el solucionador de DNS.
Resolución IP	La dirección IP del solucionador DNS desde el que nuestra infraestructura recibió la solicitud DNS.
ASN del cliente	Número de sistema autónomo (ASN) del usuario final que generó esta medida. Por lo general, la ASN que tiene la IP del cliente.
Client IP	La IP del usuario final que generó la medición.
ID de plataforma	El ID de la plataforma del proveedor de servicios en la que se realizó la consulta.
Nombre de la plataforma	El nombre de la plataforma del proveedor de servicios en la que se realizó la consulta

Registro	Descripción
Operación correctamente realizada.	Número total de mediciones que tuvieron éxito.Consejo: Éxito/Total == Disponibilidad.
Tiempo de espera	El número de mediciones que se agotó el tiempo de espera.
Error	El número de mediciones que fueron errores.
Total	El número total de medidas.
Media	El promedio de los valores de medición para cada fila.
Mediana	El valor del percentil 50 es el valor medio de las mediciones para un proveedor en particular, cuando las mediciones se enumeran en orden.
5th	El valor del 5.º percentil para el proveedor.
10th	Valor del percentil 10 para el proveedor.
90th	Valor del percentil 90 para el proveedor.
95th	Valor del percentil 95 para el proveedor.
Stdev	La desviación estándar para el proveedor.
Disponibilidad	La disponibilidad en porcentaje para el proveedor.
Importancia	Valores sintéticos generados para ayudar a encontrar datos accionables.
Tipo de medición	El valor de medición registrado, cuyo significado varía según el tipo de sonda. Es HTTP_COLD (disponibilidad), HTTP_RTT (tiempo de ida y vuelta) o HTTP_KBPS (rendimiento).

Mejor informe anónimo para ISP

- En el informe Mejor anónimo, se utiliza un grupo de pares para la comparación “mejor”. El grupo de pares se basa en la ubicación del ISP. Por lo general, son los 10 ISP más medidos en un país específico, con un mínimo de más de 1000 sesiones.
- Los resultados del “mejor”ISP ayudan a los ISP a centrar sus esfuerzos de rendimiento en plataformas de gran volumen o críticas para el negocio y en áreas que son competitivamente débiles para sus pares.
- El informe proporciona detalles sobre el desempeño desglosado por geografía y plataforma, y lo compara con el “mejor”proveedor de servicios de Internet para los mismos criterios.

- Disponible para RTT y rendimiento.
- El siguiente es un ejemplo de mejor informe de red anónima para RTT en formato de archivo TSV.

Descripciones de registro A continuación se muestran los encabezados de las columnas y las descripciones del mejor informe anónimo. Los campos aparecen en el siguiente orden en los archivos de salida.

Registro	Descripción
Tipo de medición	El valor de medición registrado, cuyo significado varía según el tipo de sonda. Es HTTP_COLD (disponibilidad), HTTP_RTT (tiempo de ida y vuelta) o HTTP_KBPS (rendimiento).
País del cliente	País del usuario final que generó esta medida.
Región del cliente	La región del usuario final que generó esta medida.
Estado del cliente	El estado del usuario final que generó esta medida.
ID de ASN del cliente	Número de sistema autónomo (ASN) del usuario final que generó esta medida. Por lo general, la ASN que tiene la IP del cliente.
Nombre de ASN del cliente	El nombre de la ASN del usuario final que generó la medida.
País de resolución	País del solucionador DNS que gestionó la solicitud.
Región de resolución	La región del solucionador DNS que gestionó la solicitud.
Estado de resolución	El estado del solucionador DNS que manejó la solicitud.
ID de plataforma	ID de la plataforma de Service Provider a la que se intentó la consulta.
Nombre de la plataforma	Nombre de la plataforma Service Provider en la que se intentó la consulta.
Éxitos	Número total de mediciones que tuvieron éxito.Consejo: Éxito/Total == Disponibilidad.
Tiempos de espera	El número de mediciones que se agotó el tiempo de espera.
Errores	El número de mediciones que fueron errores.

Registro	Descripción
Total	El número total de medidas.
Media	El promedio de todos los valores de medición de esa fila.
Mejor Media	El mejor medio entre los 15 principales proveedores del grupo de pares.
Mediciones de la mejor media	Número total de mediciones que produjeron el mejor recuento de medias.
Mediana	El valor del percentil 50 es el valor medio de las mediciones para un proveedor en particular, cuando las mediciones se enumeran en orden.
Mejor mediana	El mejor valor del percentil 50 (por debajo del cual se encuentra el 50 por ciento de las mediciones) de los 15 principales proveedores del grupo de pares.
Mediciones de la mejor media	Número total de medidas que produjeron la mejor mediana
5th	El valor del 5.º percentil para el proveedor.
Mejor 5.º	El mejor valor del 5.º percentil de los 15 principales proveedores del grupo de pares.
Las mejores 5.ª medidas	Número total de medidas que produjeron el best_5th
10th	Valor del percentil 10 para el proveedor.
Mejor 10.º	El mejor valor del 10.º percentil de los 15 principales proveedores del grupo de pares.
Mejores 10.ª medidas	Número total de medidas que produjeron el best_10th
90th	Valor del percentil 90 para el proveedor.
Mejor 90.ª	El mejor valor del percentil 90 de los 15 principales proveedores del grupo de pares.
Las mejores medidas 90	Número total de medidas que produjeron el best_90th
95th	Valor del percentil 95 para el proveedor.
Mejor 95.ª	El mejor valor del percentil 95 de los 15 principales proveedores del grupo de pares.
Las mejores 95.ª medidas	Número total de medidas que produjeron el best_95th

Registro	Descripción
Stdev	La desviación estándar para el proveedor.
Mejor Stdev	La mejor desviación estándar de los 15 principales proveedores del grupo de pares.
Las mejores medidas de Stdev	Número total de mediciones que produjeron el mejor std.dev.
Disponibilidad	La disponibilidad en porcentaje para el proveedor. La disponibilidad es la tasa de éxito del sondeo, es decir, Éxitos/(Éxitos + Falla + Tiempos de espera)
Mejor disponibilidad	El mejor valor de disponibilidad entre los 15 principales proveedores del grupo de pares.
Mejores mediciones de disponibilidad	El número de mediciones que produjeron la mejor disponibilidad.
Importancia	Valores sintéticos generados para ayudar a encontrar datos accionables.

Descripciones del registro de temporización de navegación

Datos de sincronización de navegación

Los datos de sincronización de navegación proporcionan información sobre las diversas partes del proceso de carga de páginas para una página web.

Estos datos varían según la ubicación del usuario final, los problemas de red, los cambios realizados por el proveedor, etc. Los clientes pueden usar los datos de navigation Timing para optimizar la experiencia del usuario final al cargar la página web supervisada.

Se pueden realizar mediciones para cada sesión de Radar (si está activada). Cada sesión se adjunta a un número de ID que ayuda a realizar un seguimiento de todas las mediciones de una sesión. Estas mediciones se comparten con los clientes como Registros de sincronización de navegación a través de NEM.

El siguiente es un ejemplo de los datos de temporización de navegación en formato de archivo TSV.

Los siguientes son los encabezados de las columnas y las descripciones de los registros de sincronización de navegación. Los campos aparecen en el siguiente orden en los archivos de salida:

Registro	Descripción
Timestamp	Es la hora UTC de la solicitud en formato AAAA-MM-DDTHH:MI:SSZ. El valor real (hasta el segundo) en las tablas de registro se redondea a la hora más cercana (30-03-2018 T 23:00:00 Z) o al día (30-03-2018 T 00:00:00 Z) en las tablas de horas/días, respectivamente. Siempre está en UTC en todos los conjuntos de datos.
Código de respuesta	Resultado de la medición. Por ejemplo, 0: éxito, 1: tiempo de espera agotado, 4: error. Para los cálculos de disponibilidad, el porcentaje de mediciones se toma con una respuesta de 0 (éxito) frente al número total de mediciones (total). Para otros tipos de sondeos (RTT y rendimiento), el filtro solo tiene en cuenta los puntos de datos RTT con un código de éxito 0 al calcular las estadísticas en el RTT. Lo mismo para el rendimiento.
Mercado de Resolver	El mercado del solucionador DNS que manejó la solicitud. Generalmente el continente donde se encuentra el solucionador DNS, donde, 0: Desconocido (XX), 1:América del Norte (NA) 5: África (AF), 3: Europa (UE), 4: Asia (AS), 2: Oceanía (OC), 6: América del Sur (SA).
País de resolución	El país del solucionador DNS que manejó los request.ID se puede asignar a nombres enhttps://community-radar.citrix.com/ref/countries.json.gz
Región de resolución	La región del solucionador de DNS que gestionó los Request.ids se puede asignar a los nombres de https://community-radar.citrix.com/ref/regions.json.gz. No todos los países del mundo tienen regiones definidas.
Estado de resolución	El estado de la resolución de DNS que gestionó los Request.ids se puede asignar a los nombres de https://community-radar.citrix.com/ref/states.json.gz. No todos los países del mundo tienen estados definidos.

Registro	Descripción
ASN de resolución	Número de sistema autónomo (ASN) del solucionador DNS que gestionó la solicitud. Por lo general, la ASN que tiene el solucionador de DNS. Los ID se pueden asignar a nombres en https://community-radar.citrix.com/ref/asns.json.gz
Resolución IP	La dirección IP del solucionador DNS desde el que nuestra infraestructura recibió la solicitud DNS.
Mercado de clientes	El mercado del usuario final que generó esta medición. Generalmente el continente donde se encuentra la IP del cliente; donde, 0: Desconocido (XX), 1:América del Norte (NA) 5: África (AF), 3: Europa (UE), 4: Asia (AS), 2: Oceanía (OC), 6: América del Sur (SA).
País del cliente	El país del usuario final que generó esta medida. IDs se puede asignar a nombres enhttps://community-radar.citrix.com/ref/countries.json.gz
Región del cliente	La región del usuario final que generó esta medida. Por lo general, la región geográfica en la que se encuentra la IP del cliente. Los ID se pueden asignar a los nombres de https://community-radar.citrix.com/ref/regions.json.gz. No todos los países del mundo tienen regiones definidas.
Estado del cliente	El estado del usuario final que generó esta medida. Generalmente, el estado en el que se encuentra la IP del cliente. Los ID se pueden asignar a los nombres de https://community-radar.citrix.com/ref/states.json.gz. No todos los países del mundo tienen estados definidos.
ASN del cliente	Número de sistema autónomo (ASN) del usuario final que generó esta medida. Por lo general, la ASN que tiene la IP del cliente. Los ID se pueden asignar a nombres en https://community-radar.citrix.com/ref/asns.json.gz

Registro	Descripción
Client IP	La IP del usuario final que generó la medición.
Anfitrión de Referente	La información del Referer (Protocolo, Host y Ruta) proviene del encabezado del Referer de la solicitud HTTP a Radar.
Protocolo de referencia	La información del Referer (Protocolo, Host y Ruta) proviene del encabezado del Referer de la solicitud HTTP a Radar.
Ruta de referencia	La información del Referer (Protocolo, Host y Ruta) proviene del encabezado del Referer de la solicitud HTTP a Radar.
Categoría de dispositivo	Todos los dispositivos se clasifican en uno de los siguientes: Smartphone, Tablet, PC, Smart TV y Otros. 'Otro'se utiliza como valor predeterminado si el analizador no puede determinar el valor de cualquiera de los campos.
Dispositivo	El tipo de dispositivo en el que se encuentra el usuario, por ejemplo, un iPhone de Apple. La cadena del agente de usuario lo detecta desde el explorador que se ejecuta en la página que aloja la etiqueta Radar.
Explorador web	El tipo de explorador que está utilizando el usuario, por ejemplo Mobile Safari UI/WKWebView 0.0.0. La cadena del agente de usuario lo detecta desde el explorador que se ejecuta en la página que aloja la etiqueta Radar.
SO	El sistema operativo que se está utilizando, por ejemplo iOS 11.0.3. La cadena del agente de usuario lo detecta desde el explorador que se ejecuta en la página que aloja la etiqueta Radar.
Hora de búsqueda de DNS	Con la API Resource Timing, se calcula la diferencia entre el final de la búsqueda de dominio y el inicio de la búsqueda de dominio. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como domainLookupEnd - domainLookupStart.

Registro	Descripción
Hora de conexión TCP	Con la API Resource Timing, se calcula la diferencia entre Connect End y Connect Start. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como connectEnd - connectStart.
Tiempo de conexión seguro	Con la API Resource Timing, se calcula la diferencia entre el fin de la conexión y el inicio de la conexión segura. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como connectEnd - secureConnectionStart.
Load (evento)	Es la duración o el tiempo que se tarda en ir desde el principio hasta el final del evento load. Se calcula como loadEventEnd - loadEventStart, cuando ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio.
Redirigir	Es la duración o el tiempo que se tarda en pasar de Inicio de navegación a Inicio de búsqueda. Se calcula como FetchStart - navigationStart, cuando ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio.
Carga total de página	Es la duración o el tiempo que se tarda en pasar desde el inicio de la navegación hasta el final del evento de carga de página. Se calcula como - Cargar fin de evento - Inicio de navegación cuando ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio.
dom	La duración o el tiempo que se tarda en pasar de la carga dom a dom completado. Se calcula como DomComplete - DomLoading cuando ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio.

Registro	Descripción
Latencia	Con la API Resource Timing, se calcula la diferencia entre el inicio de la respuesta y el inicio de la solicitud. Calcula cuándo ambos valores no son nulos y la hora de inicio de la respuesta es mayor que la hora de inicio de la solicitud. Se calcula como responseStart - requestStart
Tiempo de descarga	Con la API Resource Timing, se calcula la diferencia entre el final de la respuesta y el inicio de la respuesta. Calcula cuándo ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio. Se calcula como responseEnd - responseStart.
dom interactivo	La duración o el tiempo que se tarda en pasar de Inicio de navegación a dom Interactive. Se calcula como DomInteractive - navigationStart cuando ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio.
Iniciar modelizado	La duración o el tiempo que se tarda en pasar de Inicio de navegación a Iniciar procesamiento. Se calcula como startRender - navigationStart cuando ambos valores no son nulos y la hora de finalización es mayor que la hora de inicio.

Registros Openmix y HTTP Openmix

Los registros Openmix y HTTP Openmix permiten a los clientes utilizar mediciones en tiempo real para supervisar el comportamiento de sus aplicaciones Openmix. Pueden usar estos datos para encontrar áreas de mejora o para verificar el rendimiento esperado de sus aplicaciones.

- Estos registros proporcionan mediciones en tiempo real tomadas para los clientes de Openmix.
- El formato de archivo recomendado para estos registros es JSON, pero también están disponibles en formato TSV.
- A continuación se muestran ejemplos de datos de uso compartido de registros Openmixy HTTP Openmix en formato de archivo TSV.

Descripciones del registro de Openmix

Registro	Descripción
Timestamp	Es la hora UTC de la solicitud en formato AAAA-MM-DDTHH:MI:SSZ. El valor real (hasta el segundo) en las tablas de registro se redondea a la hora más cercana (30-03-2018 T 23:00:00 Z) o al día (30-03-2018 T 00:00:00 Z) en las tablas de horas/días, respectivamente. La marca de tiempo siempre está en UTC en todos los conjuntos de datos.
ID de zona del propietario de la aplicación	El identificador de zona del propietario de la aplicación que atiende la solicitud. Este valor es siempre igual a 1.
ID de cliente del propietario de la aplicación	El ID de cliente del propietario de la aplicación que atiende la solicitud. Para las solicitudes HTTP, codifique este ID en la ruta de la solicitud y utilícelo para buscar qué aplicación ejecutar.
ID de aplicación	El ID de la aplicación en la cuenta del cliente que atiende la solicitud. Este ID también está codificado en la ruta de solicitud HTTP. Los ID de aplicación comienzan en 1 y solo son exclusivos del cliente. Debe calificar completamente las consultas para un ID de aplicación específico consultando en appOwnerCustomerId.

Registro	Descripción
Versión de la aplicación	Versión de la aplicación que atendía la cuenta. Cada vez que una aplicación se actualiza a través del portal o la API, la versión se incrementa. Se registra la versión que se estaba ejecutando en el momento de la solicitud. Esta información se puede utilizar para separar la lógica versionada a lo largo del tiempo a medida que se actualizan las aplicaciones. Los hosts de toda la red generalmente reciben actualizaciones en un período de tiempo similar, pero casi nunca exactamente en el mismo momento. Es probable que las decisiones superpuestas en el tiempo utilicen diferentes versiones de una aplicación durante el proceso de actualización.
Nombre de la aplicación	El nombre de la aplicación que atendía la cuenta.
Mercado	El mercado del usuario final que generó esta medición.
País	País del usuario final que generó esta medida.
Región	La región del usuario final que generó esta medida.
State	El estado del usuario final que generó esta medida.
ID de ASN	Número de sistema autónomo (ASN) del usuario final que generó esta medida. Por lo general, el número de sistema autónomo que tiene la IP del cliente.
Nombre de ASN	El nombre de la ASN del usuario final que generó la medida.

Registro	Descripción
IP efectiva	La IP efectiva es la IP utilizada para procesar la solicitud. Es la IP especificada por cadena de consulta que anula la IP solicitante (frente a The Resolver/ECS/EDNS ID para el flujo DNS). Es la dirección que el sistema considera el objetivo al procesar la información. Esta IP es la IP del solucionador solicitante o la dirección IP de ECS del cliente si se admite EDNS ECS. Por lo tanto, todos los datos de rendimiento de la sonda, información geográfica, etc.pasados a la lógica de la aplicación se basan en esta IP.
Mercado de Resolver	El mercado del solucionador DNS que manejó la solicitud.
País de resolución	País del solucionador DNS que gestionó la solicitud.
Región de resolución	La región del solucionador DNS que gestionó la solicitud.
Estado de resolución	El estado del solucionador DNS que manejó la solicitud.
ID de ASN del solucionador	Número de sistema autónomo (ASN) del solucionador DNS que gestionó la solicitud. Por lo general, el número de sistema autónomo que tiene el solucionador de DNS.
Nombre ASN del solucionador	El nombre de la ASN del solucionador que gestionó la solicitud.
Resolución IP	La dirección IP del solucionador DNS desde el que nuestra infraestructura recibió la solicitud DNS.
Nombre del proveedor de decisiones	Alias de la plataforma que selecciona una aplicación.
Código de motivo	Código de razón establecido dentro de la aplicación que describe el motivo detrás de la decisión.
Registro de motivos	Este registro es un resultado definido por el cliente de la aplicación Openmix. Es un campo de cadena de caracteres opcional que permite a los clientes registrar información sobre sus decisiones sobre la aplicación Openmix.

Registro	Descripción
Modo de reserva	Este modo indica si la aplicación estaba en modo alternativo cuando gestionó la solicitud. El retroceso ocurre cuando algo falló durante la preparación de la solicitud de ejecución.
Usado EDNS	True si la aplicación usa una extensión de subred del cliente de EDNS.
TTL	El TTL (Time To Live) que fue devuelto.
Respuesta	El CNAME devuelto de la solicitud.
Resultado	El valor de este campo siempre es 1.
Contexto	Es el resumen de los datos de Radar que estaban disponibles para Openmix cuando se gestionó la solicitud. Openmix resuelve los datos de Radar en relación con los valores efectivos de cada solicitud, por lo que dos clientes que realizan solicitudes al mismo tiempo pueden tener diferentes cadenas de contexto.

Descripciones del registro de API HTTP de Openmix

Registro	Descripción
Timestamp	Es la hora UTC de la solicitud en formato AAAA-MM-DDTHH:MI:SSZ. El valor real (hasta el segundo) en las tablas de registro se redondea a la hora más cercana (30-03-2018 T 23:00:00 Z) o al día (30-03-2018 T 00:00:00 Z) en las tablas de horas/días, respectivamente. La marca de tiempo siempre está en UTC en todos los conjuntos de datos.
ID de zona del propietario de la aplicación	El identificador de zona del propietario de la aplicación que atiende la solicitud. Este valor es siempre igual a 1.
ID de cliente del propietario de la aplicación	El ID de cliente del propietario de la aplicación que atiende la solicitud. Para las solicitudes HTTP, codifique este ID en la ruta de la solicitud y se usa para buscar qué aplicación ejecutar.

Registro	Descripción
ID de aplicación	El ID de la aplicación en la cuenta del cliente que atiende la solicitud. Este ID también está codificado en la ruta de solicitud HTTP. Los ID de aplicación comienzan en 1 y solo son exclusivos del cliente. Debe calificar completamente las consultas para un ID de aplicación específico consultando en appOwnerCustomerId.
Versión de la aplicación	Versión de la aplicación que atendía la cuenta. Cada vez que una aplicación se actualiza a través del portal o la API, la versión se incrementa. Se registra la versión que se estaba ejecutando en el momento de la solicitud. Esta información se puede utilizar para separar la lógica versionada a lo largo del tiempo a medida que se actualizan las aplicaciones. Los hosts de toda la red generalmente reciben actualizaciones en un período de tiempo similar, pero casi nunca exactamente en el mismo momento. Es probable que las decisiones superpuestas en el tiempo utilicen diferentes versiones de una aplicación durante el proceso de actualización.
Nombre de la aplicación	El nombre de la aplicación que atendía la cuenta.
Mercado	El mercado del usuario final que generó esta medición.
País	País del usuario final que generó esta medida.
Región	La región del usuario final que generó esta medida.
State	El estado del usuario final que generó esta medida.
ID de ASN	El ID del número de sistema autónomo (ASN) del usuario final que generó esta medición, es decir, el número de ID de red asociado al nombre de ASN
Nombre de ASN	El nombre de la ASN del usuario final que generó la medida.

Registro	Descripción
IP efectiva	La IP efectiva es la IP utilizada para procesar la solicitud. Es la IP especificada por cadena de consulta que anula la IP solicitante (frente a The Resolver/ECS/EDNS ID para el flujo DNS). Es la dirección que el sistema considera el objetivo al procesar la información. Esta IP es la IP del solucionador solicitante o la dirección IP de ECS del cliente si se admite EDNS ECS. Todos los datos de rendimiento de la sonda, la información geográfica, etc., que se pasan a la lógica de la aplicación se basan en esta IP.
Nombre del proveedor de decisiones	Alias de la plataforma que selecciona una aplicación.
Código de motivo	Código de razón establecido dentro de la aplicación que describe el motivo detrás de la decisión.
Registro de motivos	Este registro es un resultado definido por el cliente de la aplicación Openmix. Es un campo de cadena de caracteres opcional que permite a los clientes registrar información sobre sus decisiones sobre la aplicación Openmix.
Modo de reserva	Este modo indica si la aplicación estaba en modo alternativo cuando gestionó la solicitud. El retroceso ocurre cuando algo falló durante la preparación de la solicitud de ejecución.
Código de respuesta	Resultado de la medición. Por ejemplo, 0: éxito, 1: tiempo de espera agotado, 4: error. Para los cálculos de disponibilidad, el porcentaje de mediciones se toma con una respuesta de 0 (éxito) frente al número total de mediciones (total, independientemente de la respuesta). Para otros tipos de sonda (RTT y rendimiento), el filtro solo debe tener en cuenta los puntos de datos RTT con un código de éxito 0 al calcular las estadísticas en el RTT. Lo mismo para el rendimiento.

Registro	Descripción
HTTP (método)	El método HTTP (get/post/options/etc) se refiere a la solicitud que se realizó al servidor HTTP Openmix desde un servicio de atención al cliente. Juntos, estos métodos forman partes de la URL entrante y las respuestas HTTP salientes.
URI	Es la ruta de solicitud. Si los clientes no obtienen el comportamiento que desean, puede deberse a una solicitud mal estructurada. Los registros muestran lo que reciben nuestros servidores (protocolo, host y ruta). La información del Referer (Protocolo, Host y Ruta) proviene del encabezado del Referer de la solicitud HTTP a Radar. Para HTTP OPX, el Referer completo (protocolo, host y ruta) se incluye en una cadena etiquetada Referer.
Agente de usuario	Es la cadena del agente de usuario de la página del explorador que aloja la etiqueta. Por ejemplo, si usa Chrome y navegas por una página con la etiqueta Radar, las mediciones de radar en segundo plano registran el agente de usuario de su explorador Chrome. Las medidas incluyen el explorador Chrome, la versión de Chrome, información sobre el sistema operativo en el que se ejecuta Chrome, etc.
Contexto	Es el resumen de los datos de Radar que estaban disponibles para Openmix cuando se gestionó la solicitud. Openmix resuelve los datos de Radar en relación con los valores efectivos de cada solicitud, por lo que dos clientes que realizan solicitudes al mismo tiempo pueden tener diferentes cadenas de contexto.

Informes personalizados para organizaciones de terceros

Los clientes pueden trabajar con NetScaler para obtener informes personalizados basados en los datos de Radar que recopila NetScaler. NetScaler puede generar informes para ejecutarlos según un cronograma. Los informes están disponibles como archivos de datos, normalmente en formato

TSV.

Preguntas frecuentes

Radar

¿Con qué frecuencia se envían archivos a S3 y GCS? La frecuencia de los depósitos de archivos es una vez por minuto para Radar y diariamente para los informes.

¿Dónde se almacenan los informes? S3 Legado (Ubicación 1):

```
s3://public-radar/[customer name]/
```

S3 (Ubicación 2):

```
s3://cedexis-netscope/[customer id]/
```

GCS (Ubicación 3):

```
gs://cedexis-netscope-[customer id]/
```

¿Cómo obtener las credenciales de acceso a S3 si aún no las tiene? El portal proporciona una clave de "Acceso"y "Secreta". Utilice las claves con 's3cmd', 'awscli'u otras herramientas para acceder a S3. Para Google Storage, el Portal descarga un archivo con credenciales de acceso para usarlo con la herramienta "gsutil".

¿Cómo usar las claves de acceso y secretas con s3cmd para descargar registros e informes del depósito S3? En primer lugar, tendría que descargar e instalar el`s3cmd` desdehttps://s3tools.org/download, y consultar elhttps://s3tools.org/usage uso, las opciones y los comandos. A continuación, ejecute el siguiente comando:

```
s3cmd --access_key=[access key] --secret_key=[secret key] ls s3://
    cedexis-netscope/<customer id>/radar/
<!--NeedCopy-->
```

Para descargar los archivos, ejecute el siguiente comando:

```
s3cmd --access_key=[access_key] --secret_key=[secret_key] get s3://
    cedexis-netscope/<customer id>/radar/[the_filename_to_download] [
    the_name_of_the_local_file]
<!--NeedCopy-->
```


Cómo usar la configuración s3cmd para enumerar archivos en el depósito S3 El primer paso es instalar`s3cmd`. Puede instalarlo desdehttp://s3tools.org/download

Para configurar s3cmd, ejecute el siguiente comando

```
s3cmd ls s3://cedexis-netscope/[customer id]/
<!--NeedCopy-->
```

Si ya está utilizando`s3cmd` con otro conjunto de claves de acceso y secretas, siga estos pasos:

Si ya usa `s3cmd`, haga una copia de la configuración predeterminada, en `~/.s3cfg`. Por ejemplo, haga una copia y asígnele el nombre `~/.s3cfg_netscope`. Reemplace las entradas de clave secreta y de acceso en `~/.s3cfg_netscope` por las que proporcionamos.
Utilice la nueva configuración en lugar de la predeterminada (la de su empresa) para acceder al depósito S3 con el siguiente comando:

```
s3cmd -c ~/.s3cfg_netscope ls s3://cedexis-netscope/[customer id]/
<!--NeedCopy-->
```

La principal diferencia es que tiene que poner en un`-c` y dónde está el archivo de configuración con las claves secretas y de acceso proporcionadas por Citrix.

Si quiere cambiar entre juegos de claves, insértelos en un archivo. Consulte el archivo con la opción `-c` para especificar qué par de claves está utilizando.

> **NOTA:** `-c` El parámetro indica dónde se encuentra el archivo de configuración, que contiene las claves de acceso y secreto.

Cómo usar el archivo clave con gsutil o gcloud para descargar archivos de registro Una vez descargado el archivo de clave JSON de la cuenta de servicio de Google, puede usarlo para autenticar las credenciales de su cuenta de Google, ver o descargar sus archivos de registro. Por ejemplo, esta es una forma de hacerlo con las utilidades de línea de comandos `gcloud` y `gsutil` de Google:

Paso 1: Activar el archivo de claves

Los comandos de autenticación`gcloud auth activate-` o`gsutil config -e` son necesarios para autenticar el archivo de claves para ejecutar comandos gcloud o gsutil.

Para gcloud:

Ejecute el siguiente comando con el archivo de claves descargado:

```
gcloud auth activate-service-account --key-file [downloaded config file
    ]
<!--NeedCopy-->
```

O bien:


```
gcloud auth activate-service-account --key-file=[path and file name of key file]
<!--NeedCopy-->
```

Para gsutil:

Ejecute el siguiente comando con el archivo de configuración descargado:

```
gsutil config -e
<!--NeedCopy-->
```

Paso 2: Liste los archivos en el depósito GCS (Google Cloud Storage)

Una vez que haya activado el archivo de clave de la cuenta de servicio como se describe en el paso anterior, use este comando para enumerar los archivos en el depósito de GCS:

```
gsutil ls gs://cedexis-netscope-<customer id>
<!--NeedCopy-->
```

Paso 3 (si es necesario): Restaurar credenciales originales (o cambiar entre cuentas)

Puede cambiar entre la cuenta ITM de NetScaler y otras credenciales de Google Cloud que haya autenticado de la siguiente manera.

Primero, ejecute el siguiente comando para enumerar todas sus cuentas:

```
gcloud auth list
<!--NeedCopy-->
```

A continuación, utilice el siguiente comando para cambiar a otra cuenta:

```
gcloud config set account [email of the account to switch to as shown in gcloud auth list]
<!--NeedCopy-->
```

Puede cambiar de una cuenta a otra mediante el mismo comando, reemplazando el correo electrónico por el correo electrónico de la cuenta al que quiere cambiar.

¿Cómo es el nombre del archivo? Legacy Daily:

Los nombres de ShareFile del registro diario de Radar tienen esta estructura:

`<prefix><date: YYYY-MM-DD>.<customer_id>.part<uniq_id>.kr.txt.gz`

Por ejemplo`Cedexis_Daily-2017-11-07.21222.part-cc901e1dd55eal4e.kr.txt.gz` (ejemplo no estándar)

Legado en tiempo real:

Los nombres de ShareFile de registro en tiempo real de Radar tienen esta estructura:

`<prefix><customer_id>-YYYY-MM-DDTHH:MM<uniq_id>.txt.gz`

Por ejemplo:`Cedexis_3-32291-2017-11-08T20:56-cc907e8fd71eaf4e.txt.gz`

Formato NEM Netscope:

El formato NEM Netscope para archivos compartidos de registro diario y en tiempo real tiene esta estructura:

`<freq><log_type><prefix><id_type><id><iso_dt><uniq_id>.<line_format>.gz`

Donde:

- `freq`: `"daily"| "rt"| "hr"`
- `log_type`: `"radar"| "opx"| "hopx"`
- `prefix`: `log_share.prefix`
- `id_type`: `"customer"| "provider"| "asn"`
- `id`: `log_share.match_id`
- `iso_dt`: `iso 8601 Date_time "YYYYMMDDTHHMMSSZ"`
- `uniq_id`: `hash(UUID)`
- `line_format`: `"tsv"| "json"`

Por ejemplo:`rt-radar-TestRadar1-provider-20363-20171209183034Z-cc907e8fd71eaf4e.tsv.gz`

¿Cuál es el formato del archivo de salida? Para Radar, el formato de archivo de salida es TSV (valor separado por tabulaciones), gzip.

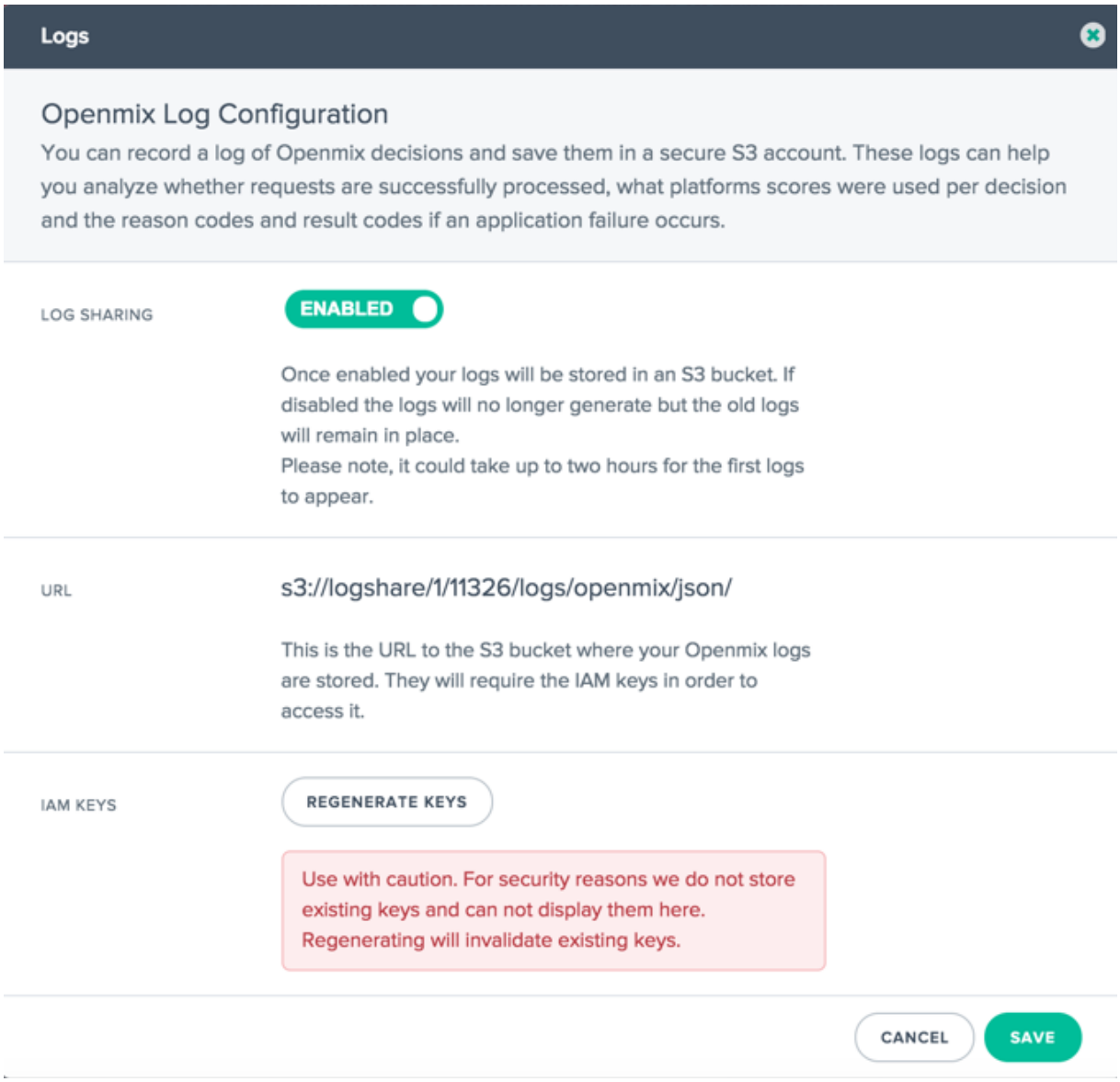
API HTTP Openmix y Openmix

¿Con qué frecuencia se envían archivos a S3? La frecuencia de los depósitos de archivos es una vez por minuto para Openmix y HTTP Openmix.

¿Qué pasa si no puede ver la opción para configurar el uso compartido de registros en tiempo real de las API HTTP de Openmix y Openmix? Su administrador de cuentas puede habilitar la función necesaria para configurar y habilitar el uso compartido de registros en tiempo real de la API HTTP de Openmix y Openmix.

¿Cómo se activa Openmix y una API HTTP de Openmix para compartir registros en tiempo real y acceder a los archivos? Cuando la función esté habilitada en su cuenta, verá el icono **Administrar registros**. Haga clic para abrir el cuadro de diálogo **Registros** donde puede acceder a la configuración

de Openmix Log Configuration. Estas configuraciones son básicamente todo lo que necesita para activar Openmix y HTTP Openmix en tiempo real para compartir registros y acceder a los archivos.



¿Cuál es el proceso back-end? Al activar el uso compartido de registros de Openmix, también se habilita el uso compartido de registros de la API HTTP de Openmix. Los servicios de uso compartido de registros de API HTTP Openmix y Openmix deben comenzar a generar registros para el cliente en 10 minutos.

¿Dónde se almacenan los informes Openmix y HTTP Openmix? S3 Legado (Ubicación 1):

```
s3://logshare/[zone ID]/[customer ID]/logs/openmix/json/[YYYY]/[MM]/[DD]/[HH]/.
```


S3 (Ubicación 2):

```
s3://cedexis-netscope/[customer id]/
```

GCS (Ubicación 3):

```
gs://cedexis-netscope-[customer id]/
```

¿Cómo es el nombre del archivo? La estructura de nombres de archivo para Openmix y HTTP Openmix normalmente se ve así:

Legado en tiempo real:

```
[zone ID, 1][customerID]-openmix-json[YYYY][MM][DD][HH][mm][ss]Z-m1-w9-c0.gz
```

Formato NEM Netscope:

El formato NEM Netscope para archivos compartidos de registro diario y en tiempo real tiene esta estructura:

```
<freq><log_type><prefix><id_type><id><iso_dt><uniq_id>.<line_format>.gz
```

Donde:

- `freq`: `"daily"| "rt"| "hr"`
- `log_type`: `"radar"| "opx"| "hopx"`
- `prefix`: `log_share.prefix`
- `id_type`: `"customer"| "provider"| "asn"`
- `idv`: `log_share.match_id`
- `iso_dt`: `iso 8601 Date_time "YYYYMMDDTHHMMSSZ"`
- `uniq_id`: `hash(UUID)`
- `line_format`: `"tsv"| "json"`

Por ejemplo:`hr-opx-TestOpenmix1-provider-20363-20171209183034Z-cc907e8fd71eaf4e.tsv.gz`

¿Cuál es el formato de archivo de salida? El formato de archivo para Openmix y una API HTTP de Openmix es JSON (comprimido con gzip).

Administración

September 13, 2023

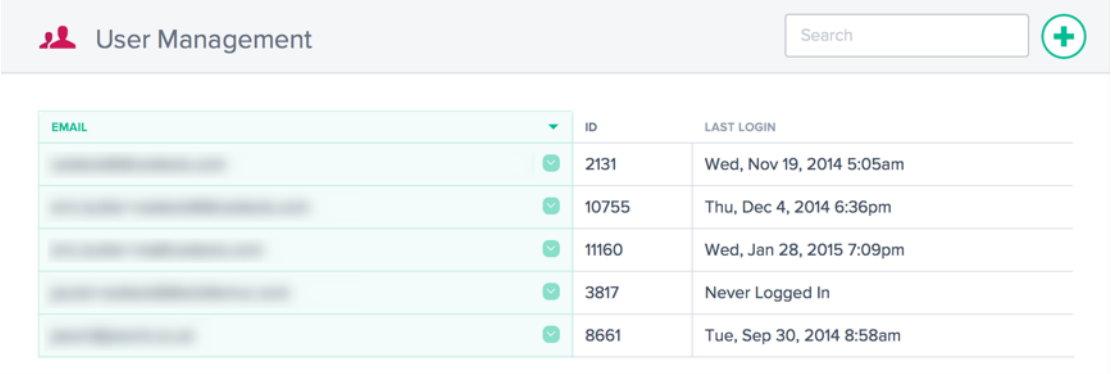
La sección **Mi cuenta** es donde el usuario final puede administrar la cuenta, los usuarios que pueden acceder a ella y los usuarios que pueden acceder a las funciones de depuración de Fusion.

Además, desde el menú puede ver las facturas vencidas y administrar las credenciales de la API de OAuth.

Administrar usuarios

En el menú Usuarios puede agregar o quitar usuarios y restablecer el acceso a la cuenta con contraseña.

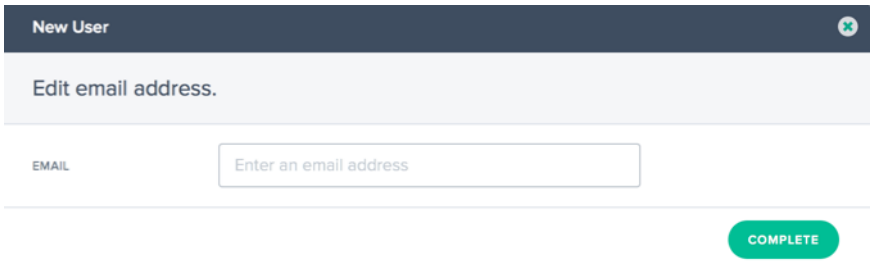
Además de la gestión de usuarios, puede introducir direcciones de correo electrónico para las notificaciones de servicio y ver cuándo un usuario ha iniciado sesión por última vez.



Agregar o quitar usuarios y restablecer contraseñas

Al crear o agregar usuarios, asegúrese de utilizar una dirección de correo electrónico válida. Las contraseñas se crean automáticamente y se envían por correo electrónico a la dirección de correo electrónico que se introduce como nombre de usuario.

Para añadir un usuario nuevo, haz clic en el **signo +** situado en la esquina superior derecha. Introduzca una dirección de correo electrónico válida y haga clic en **Completar**.



Para restablecer la contraseña de un usuario, haga clic en la flecha hacia abajo situada a la derecha de la dirección de correo electrónico del usuario, elija **Restablecer contraseña**y confirme la acción en el cuadro de diálogo haciendo clic en **Sí**. Se envía un correo electrónico de restablecimiento de contraseña al usuario.

Se puede eliminar un usuario del sistema haciendo clic en la flecha hacia abajo situada a la derecha de la dirección de correo electrónico del usuario y seleccionando **Eliminar**. Confirme la acción y el usuario será eliminado del sistema.

Single Sign-On

Apoyamos el uso de proveedores de identidad de terceros para Single Sign-On en el Portal a través de SAML 2.0.

Single Sign-On se utiliza para la autenticación de inicios de sesión de usuario. Actualmente no transferimos la información de autorización a través de SAML SSO. Para poder iniciar sesión, un usuario debe existir en el portal de administración inteligente del tráfico de NetScaler con la misma dirección de correo electrónico que un usuario del proveedor de identidades de SSO.

Single Sign-On se administra por cuenta. Una vez activado Single Sign-On para una cuenta, todos los usuarios deben utilizar un inicio de sesión único para acceder al Portal.

Encontrará la información de configuración de SAML en el elemento de menú **Configuración de SSO**. La información es específica de su cuenta y le permite configurar Single Sign-On en su proveedor de identidades. Si no encuentra el menú de **configuración del SSO**, póngase en contacto con el equipo de soporte .

La configuración es diferente para cada proveedor de identidad, pero necesita la siguiente información, que se muestra en la página Configuración de SSO:

- URL del servicio al consumidor de aserción (ACS)
- ID de entidad
- URL de cierre de sesión (opcional, dependiendo del proveedor)
- URL de inicio (opcional, dependiendo del proveedor)
- Formato de nombre: Correo electrónico
- Respuesta firmada: No

Activar Single Sign-On

Pasos genéricos para añadir el inicio de sesión único al portal de administración inteligente del tráfico de NetScaler:

1. Utilizando los datos de la pantalla Configuración de SSO, configure el proveedor de identidades

2. Descargar el archivo de metadatos de IDP de SSO desde el proveedor de identidades
3. Cargar el archivo en la página Configuración de SSO
4. Cuando esté listo para habilitar SSO, haga clic en **Habilitar**
5. Los usuarios tendrán que iniciar sesión a través de la página de inicio de sesión SSO.

Desactivar Single Sign-On

Si SSO está configurado y habilitado, haga clic en el botón **Inhabilitar**.

Cualquier usuario de la cuenta que desee iniciar sesión deberá usar una contraseña de Citrix en la pantalla de inicio de sesión estándar. Si un usuario no conoce su contraseña, un administrador de cuenta puede enviar un correo electrónico de restablecimiento de contraseña o el usuario puede solicitar un correo electrónico de restablecimiento de contraseña desde la pantalla de inicio de sesión.

Pasos de configuración para Google G Suite

A continuación se indican los pasos necesarios para utilizar Single Sign-On con los inicios de sesión de Google G Suite:

En Google G Suite:

1. Abre la consola administrativa de G Suite en la sección Aplicaciones
2. Haga clic en la categoría **Aplicaciones SAML**
3. Haga clic en el botón **Habilitar inicio de sesión único para una aplicación SAML**
4. En la parte inferior del cuadro de diálogo, elija **CONFIGURAR MI OWN CUSTOM APP**
5. En el cuadro de diálogo Información del proveedor de identidades de Google, descargue el archivo de metadatos del proveedor de identidades en Opción 2.
6. En la información básica de su aplicación personalizada, el nombre de la aplicación puede ser «NetScaler Intelligent Traffic Management»
7. Rellene la siguiente información de la Configuración de SSO en el Portal:
   - URL ACS: desde la información de configuración de SSO
   - ID de entidad: de la información de configuración de SSO
   - URL de inicio: desde la información de configuración de SSO (opcional)
   - Nombre ID Formato: EMAIL
8. Deje vacío el cuadro de diálogo Asignación de atributos, haga clic en **Finalizar** para crear la aplicación SAML
9. En la lista Aplicaciones, haga clic en los puntos verticales a la derecha del elemento Portal y elija **ON para todos**

En el Portal:

1. En la página Configuración de SSO, sube el archivo de metadatos del IDP; haz clic en el botón **Elegir archivo**para abrir el explorador de archivos y selecciona el archivo de metadatos del IDP descargado de G Suite.
2. Si el archivo de metadatos se valida correctamente, aparece una marca de verificación verde.
3. Haga clic en **Habilitar** para habilitar Single Sign-On para todos los usuarios de la cuenta.

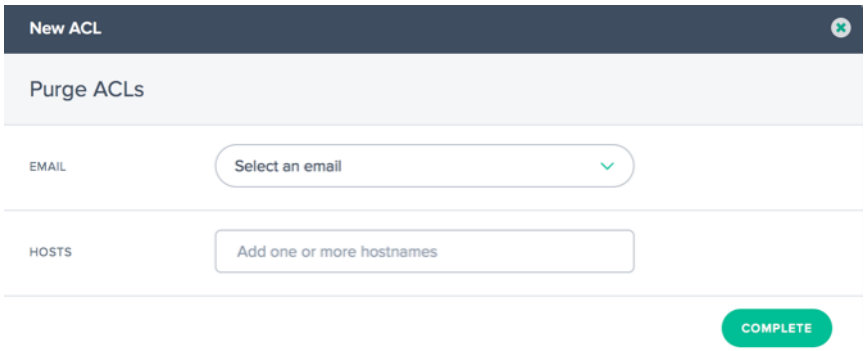
Los usuarios ahora pueden iniciar sesión en el portal de administración inteligente del tráfico de NetScaler desde la página de inicio de sesión de SSO o desdeel**menú Aplicaciones de G Suite.**

Para obtener más información sobre el SSO de Google G Suite, consulta la ayudade Google.

Configuración de ACL de depuración

En el menú **Depurar ACL**, los usuarios pueden tener limitaciones en su capacidad para ejecutar la funcionalidad Depuración de Fusion. De forma predeterminada, los usuarios pueden ejecutar una depuración en cualquier host configurado en la configuración de **Depuración de Fusion**. Las ACL de depuración se utilizan para limitar a los usuarios a permitir solo una depuración en los hosts especificados.

Agregue nuevas restricciones para un usuario haciendo clic en el botón **'+'** en la esquina superior derecha. Aparece el siguiente cuadro de diálogo:



Campo	Descripción
Correo electrónico	Seleccione el correo electrónico del usuario al que desea configurar el acceso de depuración limitado.
Anfitriones	Introduzca los nombres de host para que el usuario ejecute las purgas. Los nombres de host no incluidos en la lista para el usuario no estarán disponibles para su depuración por el usuario.

Facturas

La opción de menú **Facturas** proporciona todas las facturas de los servicios de NetScaler Intelligent Traffic Management que ha consumido. Si hay algún problema con las facturas, póngase en contacto con su representante de ventas o, si lo prefiere, póngase en contacto con el equipo de soporte .

API

Administrar OAuth

La opción del menú **API** proporciona detalles sobre los tokens de API de OAuth autenticados que desee usar. Si desea utilizar esta funcionalidad, póngase en contacto con su administrador de cuentas.

Límites de velocidad de API REST

Las API REST se pueden utilizar para acceder a los datos y configuraciones almacenados en la plataforma. Sin embargo, limitamos el número de solicitudes (para acceder a estos datos) poniendo un límite de tarifa en ellas, es decir, limitamos el número de llamadas API que un cliente puede realizar en un período de tiempo determinado. Esto se hace para equilibrar la carga en el sistema.

Atributos de límite de velocidad Los límites de velocidad tienen los siguientes atributos:

- Rango de tiempo (en minutos)
- Número de solicitudes permitidas
- Solicitudes simultáneas

Los clientes pueden solicitar aumentos en sus límites de tarifas para su caso de uso específico.

Límites de velocidad predeterminados En la tabla siguiente se enumeran los diferentes tipos de llamadas a la API y los límites de velocidad predeterminados que se aplican a cada una de ellas.

Tipos de API	Límites de velocidad predeterminados
Puntos finales de informes	**GET**

`/v2/reporting/radar.json`
`/v2/reporting/plt.json`
`/v2/reporting/openmix.json`
`/v2/reporting/sonar.json`
	15 solicitudes por 15 minutos. 3 solicitudes simultáneas

Tipos de API	Límites de velocidad predeterminados
Actualización de aplicaciones	**PONER, PUBLICAR**
`/v2/config/applications/dns.json`	10 solicitudes por minuto. 3 solicitudes simultáneas
Depuración de Fusion	**GET**
`/v2/actions/fusion/purge.json`	150 solicitudes por minuto
Depuración de Fusion	**POST**
`/v2/actions/fusion/purge.json`	1 solicitud por minuto. 3 solicitudes simultáneas